Manual de Corporativas Vinculantes/ BCR Manual/

Controller and processor Rules

Nota: Este Manual contiene las BCR aplicables a Concentrix tanto como encargado y responsables, respectivamente.

Note: This Manual contains the applicable BCR to Concentrix as Controller and Processor, respectively.

Note: (Este Manual contém o BCR aplicável à Concentrix como Controlador e Processador, respectivamente.

Normas corporativas vinculantes en calidad de responsable

Nuestras BCRs para el Responsable se aplica únicamente a la filial de Concentrix bajo Webhelp SAS, que actúa como Entidad Europea Principal.

Las filiales a las que se aplican las BCR se enumeran en el Apéndice 01 de las BCR.

concentrix

Contenido

1. Introducción

Recordatorio: Tras la transacción entre Webhelp y Concentrix en septiembre del 2023, el nombre comercial del grupo es ahora Concentrix. Sin embargo, es importante tener en cuenta que el alcance de las presentes BCR no se ha modificado. Las BCR sólo son aplicables a las Afiliadas de Webhelp SAS que actúen como Entidad Europea Principal. Las afiliadas que están sujetas a las BCR (Responsable y/o Encargado) se enumeran en el Apéndice 01 y se las denominará Miembros de las BCR.

En el Grupo Concentrix, creemos que la protección de los Datos personales no es sólo una cuestión de seguridad o cumplimiento de un marco legal particular, sino un compromiso individual y organizacional. La divulgación y el intercambio de los estándares de Concentrix a través de las Normas Corporativas Vinculantes para Encargados (en adelante, las "BCR-P") y las presentes Normas Corporativas Vinculantes para Responsables (en adelante, las "BCR-C") es de suma importancia en relación con las expectativas legítimas de los Titulares de los Datos sobre cómo se Procesan sus Datos personales.

En el curso de sus actividades, los Miembros de las BCR procesan tanto Datos Personales internos como de Clientes. En este sentido, los Miembros de las BCR protegen los Datos personales que procesan en su nombre mediante la implementación de medidas y controles técnicos, físicos y administrativos adecuados, comprendidos en las presentes BCR-C. Dichos controles garantizarán que toda la organización Procese Datos personales de manera consistente, independientemente de la naturaleza y/o el lugar del Procesamiento.

Este enfoque es particularmente importante debido a la diversidad de actividades que Concentrix cubre en nombre de sus Clientes.

Como consecuencia de lo anterior y teniendo en cuenta los requisitos introducidos por el Reglamento Europeo 2016/679 adoptado el 27 de abril de 2016 (en adelante, el "**Reglamento de la UE**" o "**RGPD**") y las normas, reglamentos y leyes aplicables en el ámbito de la protección de datos, siempre que no contravengan el Reglamento de la UE, los Miembros de las BCR Procesarán Datos personales de acuerdo con los siguientes principios:

- **Licitud** – Los Datos personales se recogerán y procesarán cuando el Titular de los Datos haya dado su consentimiento para el Procesamiento o cuando el Procesamiento sea legítimo o necesario de conformidad con la Legislación Aplicable sobre Protección de Datos;
- **Lealtad** – el tratamiento de Datos personales debe tener en cuenta las circunstancias específicas y el contexto en el que se procesan dichos Datos personales;
- **Transparencia** – la información y la comunicación relacionadas con el Tratamiento de Datos personales deben ser fácilmente accesibles, fáciles de entender, claras y en un lenguaje sencillo y claro;
- **Limitación de la finalidad** – los Datos personales se recolectarán con fines específicos, explícitos y legítimos y no se procesarán posteriormente de una manera que sea incompatible con dichos fines;

- **Minimización de datos** – los Datos personales recolectados serán adecuados, relevantes y limitados a lo necesario en relación con los fines para los que se procesan;
- **Exactitud** – los Datos personales serán exactos y cuando sea necesario se mantendrán actualizados. Se deben tomar todas las medidas razonables para garantizar que los Datos personales que sean inexactos, teniendo en cuenta los fines para los cuales se procesan, se eliminados o rectificados sin demora indebida;
- **Limitación de almacenamiento** – los Datos personales deben mantenerse en una forma que permita la identificación de los Titulares de Datos por no más tiempo del necesario para los fines para los que se procesan o cualquier otra retención legal;
- **Integridad y confidencialidad** – los Datos personales se procesarán de manera que se garantice la seguridad adecuada, incluida la protección contra el procesamiento no autorizado o ilícito y contra la pérdida, destrucción o daño accidental, utilizando medidas técnicas, físicas y administrativas apropiadas.

A través de estas BCR-C, Concentrix tiene la intención de compartir y especificar los detalles y los principios aplicables a todos los Miembros de las BCR y proporcionar ciertos estándares para todo el grupo que permitan la implementación de las BCR-C. Además, Concentrix puede poner a disposición políticas específicas, locales o sectoriales. En caso de que exista una contradicción entre estas BCR-C y dichas políticas específicas, locales o sectoriales, prevalecerán los términos de las BCR-C, a menos que las disposiciones contradictorias de dichas políticas específicas, locales o sectoriales protejan mejor los derechos y la libertad del Titular de los Datos.

Dado que las BCR-C tienen como objetivo garantizar un enfoque adecuado y consistente en toda la organización de Concentrix con respecto al Procesamiento de Datos personales, las excepciones que podrían resultar de las legislaciones aplicables no se reflejan en estas BCR-C. Sin embargo, estas BCR-C incluyen un mecanismo de notificación en la sección 12.3 donde la legislación nacional impide que un Miembro de las BCR cumpla con las BCR-C y cuando los Estados Miembros de la UE proporcionan reglas específicas adicionales al Reglamento de la UE. En consecuencia, la legislación local se considerará una excepción aplicable a estas BCR-C y se registrará en consecuencia, tras la notificación correspondiente. Como se especifica en la sección 12.3, cuando esta legislación nacional imponga un nivel más alto de protección de los Datos Personales, esta legislación nacional prevalecerá sobre las BCR-C.

2. Alcance

2.1 Alcance del material

Esta BCR-C es aplicable siempre que un Miembro de las BCR Procese Datos Personales como Responsable de los datos y como Encargado de los datos para Procesamiento realizado dentro de la organización de Concentrix, a nombre de un Miembro de las BCR que actúe como Responsable de los datos.

Debido a la diversa gama de actividades que cubre Concentrix, Concentrix puede tener que procesar varias categorías en constante evolución de Datos Personales, tales como:

- Información relacionada con la vida personal (por ejemplo, gestión de reclutamiento, sistema de grabación de cámaras, gestión de clientes y prospectos);
- Información económica y financiera (por ejemplo, gestión de nóminas, gestión de clientes y prospectos);
- Información de identificación (por ejemplo, gestión de proveedores, comunicación no comercial, encuestas y formularios, gestión de clientes y prospectos);
- Información técnica (por ejemplo, gestión de TI y telefonía, gestión de credenciales, gestión de registros de empleados); o
- Información transaccional (por ejemplo, gestión de entidades corporativas y legales).

El alcance del material se detalla con mayor precisión en el **Anexo 11-A**, que proporciona una tabla detallada sobre el Propósito del Procesamiento y las categorías relacionadas de Titulares de la información y de Datos Personales cubiertas por el presente BCR-C. **El Anexo 01** proporciona información sobre los países terceros y los Miembros de las BCR a los que se transfiere Datos Personales.

El BCR-C se aplicará a todos los Titulares de la información cuya Datos Personales se transfiera dentro del ámbito de aplicación del BCR-C desde un Miembro de las BCR bajo el ámbito de aplicación del RGPD. Por lo tanto, el Miembro de las BCR reconoce que el ámbito de aplicación del BCR-C puede, no limitarse a "ciudadanos o residentes del EEE".

Además, este BCR-C se aplica al Procesamiento de Datos Personales por un Miembro de las BCR que actúe como Responsable de los datos o como Encargado de los datos en nombre de otro Miembro de las BCR que actúe como Responsable de los datos, independientemente de la categoría y naturaleza de dicha Datos Personales.

Adicionalmente, cada Miembro de las BCR es también el Responsable de los datos de los Datos Personales de sus empleados como su empleador. Al Procesar Datos Personales de sus empleados, los Miembros de las BCR cumplirán con este BCR-C y Procesarán Datos Personales como se describe en la Política de Privacidad de los Empleados.

2.2 Alcance Geográfico

Concentrix desea implementar, en la medida de lo posible, un enfoque coherente dentro de la organización donde se procese Datos Personales. En consecuencia, todos los Miembros de las BCR, independientemente de su ubicación o jurisdicción legal, están sujetos a este BCR-C. Por lo tanto, el presente BCR-C se aplicará al menos a toda los Datos Personales transferida a Miembros de las BCR fuera del EEE, y a las transferencias ulteriores a otros Miembros de las BCR fuera del EEE. Cabe recordar que las entidades de Concentrix vinculadas por el presente BCR-C (es decir, los Miembros de las BCR) están enumeradas en el Anexo 01.

Como principio, ninguna Transferencia de Datos Personales será realizada por ninguna entidad de Concentrix a menos que y hasta que esté vinculada por este BCR-C a una entidad de Concentrix no vinculada por este BCR-C. Cualquier Transferencia de este tipo no podrá llevarse a cabo a menos que esta afiliada de Concentrix haya proporcionado garantías suficientes para implementar medidas técnicas y organizativas apropiadas de manera que el Procesamiento y las obligaciones vinculadas a dicho Procesamiento cumplan con los requisitos de este BCR-C y aseguren la protección de los derechos de los Titulares de la información.

El Miembro de las BCR vinculado por el BCR-C y las entidades de Concentrix no vinculadas suscribirán un acuerdo escrito para garantizar esto.

3. Naturaleza Vinculante

3.1 Sobre los empleados de Concentrix

Cada empleado de un Miembro de las BCR, como Titular de la información, se beneficiará de las disposiciones de este BCR-C. Dado que la protección de los Datos Personales es una cuestión de compromiso individual y organizacional, cada empleado también debe cumplir con los requisitos especificados en este BCR-C.

Como tal, el BCR-C forma parte del conjunto de políticas que los empleados de Concentrix deben cumplir como parte de su contrato de trabajo. El incumplimiento de los principios y reglas de este BCR-C puede llevar a acciones disciplinarias que podrían resultar en la terminación del contrato y en ciertas circunstancias, en cargos penales.

3.2 Sobre los Miembros de las BCR del grupo Concentrix

Como grupo, Concentrix quiere asegurarse de que todos los Miembros de las BCR que pertenecen al mismo estén vinculados de la misma o similar manera a los principios y obligaciones especificados en este BCR-C y cumplirán con los requisitos aquí especificados.

Por esta razón, este BCR-C es vinculante para todos los Miembros de las BCR mediante la firma de un Acuerdo de Transferencia de Datos Intragrupo que incluye este BCR-C como un anexo.

La lista de entidades de Concentrix vinculadas por este BCR-C se establece en el Anexo 1 de este BCR-C. Webhelp SAS, como Entidad Europea Principal, con la asistencia del DPO (por sus siglas en inglés), se compromete a mantener esta lista actualizada y disponible, y a comunicarla a las partes relevantes según se determine de vez en cuando.

3.3 Dirigido a los Encargados de los datos de Concentrix

Cuando un Miembro de las BCR contrate a un Encargado de los datos (ya sea un Miembro de las BCR, una filial del grupo Concentrix que aún no esté vinculada por el BCR o un proveedor externo) para llevar a cabo actividades específicas de Procesamiento, dicho Encargado de los datos deberá proporcionar garantías

suficientes para implementar medidas técnicas y organizativas apropiadas de manera que el Procesamiento cumpla con los requisitos de este BCR-C.

Por lo tanto, cualquier actividad de Procesamiento realizada por los Encargados de los datos de un Miembro de las BCR deberá regirse por un contrato escrito u otro acto legal vinculante y deberá establecer todos los elementos del Artículo 28 del RGPD, recordados a continuación, y en particular el objeto y la duración del Procesamiento, la naturaleza y el propósito del Procesamiento, el tipo de Datos Personales y las categorías de Titulares de la información y las obligaciones y derechos del Miembro de las BCR que actúe como Responsable de los datos.

Además, este contrato u otro acto legal vinculante con un Encargado de los datos deberá establecer las siguientes disposiciones:

1. El Encargado de los datos procesará los Datos Personales únicamente según las instrucciones documentadas del Responsable de los datos, incluso en lo que respecta a las Transferencias de Datos Personales, a menos que la ley de la Unión o del Estado Miembro a la que esté sujeto el Encargado de los datos requiera lo contrario (en tal caso, el Encargado de los datos informará al Responsable de los datos sobre dicho requerimiento legal antes de procesar, a menos que esa ley prohíba tal información por razones importantes de interés público).
2. El Encargado de los datos mantendrá los Datos Personales confidencial, asegurando especialmente que las personas autorizadas para Procesar Datos Personales se hayan comprometido a mantener la confidencialidad o estén bajo una obligación estatutaria adecuada de confidencialidad;
3. El Encargado de los datos tomará las medidas de seguridad técnicas, físicas y organizativas adecuadas para asegurar un nivel apropiado de seguridad para proteger los Datos Personales.
4. El Encargado de los datos no permitirá que el Sub-Encargado procese Datos Personales en relación con su obligación hacia un Miembro de las BCR sin la autorización previa por escrito del Miembro de las BCR y garantizará que este Sub-Encargado se comprometa a cumplir con las mismas obligaciones establecidas en el acto vinculante ejecutado entre el Encargado de los datos y el Miembro de las BCR mediante un contrato u otro acto legal conforme a la ley de la Unión o del Estado Miembro. Cuando el Sub-Encargado no cumpla con sus obligaciones de protección de datos, el Encargado de los datos inicial seguirá siendo totalmente responsable ante el Miembro de las BCR por el cumplimiento de las obligaciones de ese otro Encargado de los datos.
5. El Encargado de los datos proporcionará todo el apoyo necesario al Miembro de las BCR con respecto al manejo de las solicitudes de los Titulares de la información relacionadas con sus derechos.
6. El Encargado de los datos proporcionará toda la asistencia razonable al Miembro de las BCR para:
    - Asegurar un nivel de seguridad del Procesamiento adecuado al riesgo,
    - Sin demora indebida, informar al Miembro de las BCR de cualquier violación de seguridad real o sospechada que implique Datos

Personales y apoyar al Miembro de las BCR en la notificación a la Autoridad de Supervisión relevante y en la comunicación a los Titulares de la información afectados según sea el caso.

- Realizar una evaluación de impacto en la protección de datos (DPIA por sus siglas en inglés) y, cuando sea relevante, obtener la consulta previa con la Autoridad de Supervisión cuando la DPIA resulte en un alto riesgo en ausencia de medidas para mitigar el riesgo.

7. El Encargado de los datos cumplirá con las instrucciones del Miembro de las BCR con respecto a la eliminación o devolución de los Datos Personales al finalizar el contrato u otro acto legalmente vinculante, y eliminará las copias existentes a menos que la ley de la Unión o del Estado Miembro requiera el almacenamiento de los Datos Personales.
8. El Encargado de los datos pondrá a disposición del Miembro de las BCR toda la información necesaria para demostrar su cumplimiento y contribuirá a auditorías e inspecciones por parte de un Miembro de las BCR u otra autoridad relevante o auditor ordenado por el Miembro de las BCR.
9. El Encargado de los datos informará inmediatamente al Miembro de las BCR si, en su opinión, una instrucción infringe este BCR-C o si la Legislación de Protección de Datos Aplicable es relevante.

Cuando un proveedor y/o contratista de Concentrix procese datos personales del personal y/o contratistas de éste, deberá someterse a las reglas fijadas en el presente manual, y por tanto deberá acatar el Anexo 12 que contiene el Contrato Marco de Protección de Datos en cumplimiento de la normativa de protección de datos de la jurisdicción específica de tratamiento de la información.

4. Principios para el procesamiento de datos personales

La Legislación Aplicable de Protección de Datos define un conjunto de principios que deben observarse al Procesar Datos Personales. Concentrix se compromete a cumplir con estos principios actuando como Responsable de los datos o Encargado de los datos en nombre de un Miembro de las BCR que actúe como Responsable de los datos.

4.1 Definición de una base legal para el Procesamiento (Transparencia, equidad y licitud)

Cuando se Procesa Datos Personales, se requiere que dicho Procesamiento tenga una base legal adecuada, como las previstas en el Artículo 6 del RGPD, siendo dicha base legal el fundamento que permite el Procesamiento lícito. Los Miembros de las BCR reconocen que una de las siguientes bases legales puede ser aplicable para el Procesamiento de Datos Personales:

- Consentimiento de los Titulares de la información;
- Ejecución de un contrato en el que el Titular de la información sea parte o para la celebración de dicho contrato;
- Obligación legal establecida por la ley de la Unión o del Estado Miembro a la que esté sujeto el Responsable de los datos;

- Intereses vitales del Titular de la información u otra persona;
- Ejecución de una tarea realizada en el interés público o en el ejercicio de la autoridad oficial conferida al Responsable de los datos;
- Intereses legítimos del Responsable de los datos o de un tercero (siempre que dichos intereses no prevalezcan sobre los derechos y libertades del Titular de la información).
- O cualquier otra base legal

En este sentido, los Miembros de las BCR se comprometen a Procesar Datos Personales de manera lícita sólo cuando tengan una base legal válida para hacerlo, de acuerdo con los requisitos de la Legislación Aplicable de Protección de Datos.

Por ejemplo, el Procesamiento de los Datos Personales de los empleados de Concentrix es necesario para gestionar las solicitudes de permisos (por ejemplo, vacaciones). Así, la base legal para dicha operación de procesamiento parte de la necesidad de ejecutar el contrato de trabajo que Concentrix y sus empleados han suscrito.

Además, y en línea con el Artículo 5 a continuación, los Miembros de las BCR se comprometen a asegurar que:

- Las Categorías Especiales de Datos Personales sólo se procesen de acuerdo con una de las exenciones previstas por el Artículo 9(2) del RGPD, y
- El Procesamiento de Datos Personales relacionada con condenas penales y delitos estará prohibido, a menos que se apliquen las mismas exenciones previstas por el Artículo 10 del RGPD.

4.2 Definición de un propósito (Limitación de propósito)

A menos que esté específicamente autorizado por la Legislación de Protección de Información Aplicable, los Miembros de las BCR deberán asegurarse de haber determinado un propósito lícito, justo, explícito y legítimo antes de cualquier recolección o procesamiento de Datos Personales.

Los Miembros de las BCR se comprometen a garantizar que los propósitos que definen no infrinjan la Legislación de Protección de Información Aplicable y parezcan ser legítimos, mientras aseguran que los Datos Personales no sea procesada posteriormente de una manera incompatible con esos propósitos.

Por ejemplo, planificar la fuerza laboral necesaria para prestar sus servicios y, en consecuencia, gestionar los horarios de los empleados de Concentrix es uno de los propósitos definidos para la recolección de los Datos Personales de los empleados en relación con su solicitud de permisos.

4.3 Minimización de la recolección de Datos Personales (Minimización de datos)

Los Miembros de las BCR se comprometen a recolectar y procesar Datos Personales que sea estrictamente adecuada, relevante y limitada a lo que es necesario en relación con los propósitos para los cuales se procesa.

Los Datos Personales no deberá recolectarse ampliamente con la perspectiva de un propósito futuro no definido.

Por ejemplo, los Datos Personales recolectada para gestionar las solicitudes de permisos se limita a la naturaleza del permiso (vacaciones, licencia de maternidad, etc.) y otra información relevante (la duración del permiso), pero no incluye ninguna Datos Personales que no sea estrictamente necesaria (como con quién va de vacaciones el empleado, el destino del empleado o cualquier dato de salud para incapacidades).

4.4 Posesión de un registro

Ya sea actuando como Responsable de los datos o Encargado de los datos, los Miembros de las BCR deberán mantener un registro de todas las categorías de actividades de procesamiento de Datos Personales bajo su responsabilidad para demostrar el cumplimiento con las BCR-C.

Cuando actúe como Responsable de los datos, el Registro de Actividades de Procesamiento deberá mencionar al menos la siguiente información de acuerdo con el Artículo 30.1 del RGPD:

- El nombre y los datos de contacto de la entidad de Concentrix, el posible corresponsable y el Oficial de Privacidad de Datos;
- Los propósitos del procesamiento;
- La descripción de las categorías de Titulares de los datos y de los Datos Personales;
- Las categorías de destinatarios de los Datos Personales;
- Las posibles transferencias de Datos Personales a un país tercero o a una organización internacional;
- La duración del almacenamiento de la Información;
- Una descripción general de las medidas de seguridad técnicas y organizacionales para asegurar un nivel de seguridad adecuado al riesgo del procesamiento.

Por ejemplo, la operación de procesamiento de gestión de solicitudes de permisos de empleados se incluye en el Registro de Actividades de Procesamiento relacionado con la gestión administrativa de empleados que contiene la información listada anteriormente.

Cuando actúe como Encargado de los datos, el Registro de Actividades de Procesamiento deberá mencionar al menos la siguiente información de acuerdo con el Artículo 30.2 del RGPD:

- El nombre y los datos de contacto del o de los Encargados y de cada Responsable en cuyo nombre actúa el encargado y, cuando aplique, del representante del Responsable o del Encargado, y del DPO; Las categorías de procesamiento llevadas a cabo en nombre de cada Responsable;
- Cuando aplique, transferencias de Datos Personales a un país tercero y en su caso, las salvaguardas o exenciones aplicables de acuerdo con el Artículo 49 del RGPD.

4.5 Exactitud de los Datos Personales (Precisión de los datos)

Los Miembros de las BCR deberán implementar medidas y controles adecuados para garantizar que los Datos Personales que recolectan y procesan permanezca

precisa y, cuando sea necesario, se mantenga actualizada. Con este fin, los Miembros de las BCR se comprometen a implementar las acciones requeridas para tomar todas las medidas razonables para asegurar que los Datos Personales que sea inexacta, teniendo en cuenta los propósitos para los cuales se procesa, sea eliminada o rectificada.

Por ejemplo, los empleados tienen el deber de informar a su departamento de recursos humanos sobre cualquier actualización en su situación personal (por ejemplo, modificación de la dirección). Los Miembros de las BCR se asegurarán entonces de que los Datos Personales sea actualizada en consecuencia con el registro de los empleados.

4.6 Definición de un período de retención de datos (Período de almacenamiento limitado)

Los Miembros de las BCR no mantendrán los Datos Personales por un período más largo del estrictamente necesario, teniendo en cuenta el propósito para el cual se recolectan dichos Datos Personales. En este sentido, los Miembros de las BCR se comprometen a determinar un período de retención de datos antes de implementar cada procesamiento.

Para asegurar el cumplimiento de este requisito, los Miembros de las BCR deberán implementar un procedimiento de retención de datos y especificar las directrices a aplicar con respecto a una actividad de procesamiento determinada.

Por ejemplo, los Datos Personales recolectada para gestionar las solicitudes de permisos se mantiene el tiempo necesario para gestionar los horarios, realizar acciones relacionadas con la nómina (por ejemplo, permiso no remunerado) y cumplir con los estatutos locales aplicables de limitaciones y obligaciones contables.

4.7 Implementación de medidas de seguridad (integridad y confidencialidad)

Los Miembros de las BCR han implementado medidas y controles técnicos, físicos y administrativos apropiados para garantizar que los Datos Personales no sea accedida y/o procesada ilegalmente. Tales medidas técnicas, físicas y administrativas deben asegurar un nivel de seguridad adecuado al riesgo, incluyendo, pero no limitado a, la destrucción, pérdida, alteración, divulgación no autorizada de, o acceso a, Datos Personales transmitidos, almacenados o de otra manera procesados por cualquier Miembro de las BCR y cualquier Encargado de los datos.

Además, los Miembros de las BCR aseguran que sus subcontratistas/Encargados cumplan con las medidas de seguridad técnicas y organizacionales implementadas en Concentrix mediante la firma de acuerdos escritos con ellos que comprendan los requisitos establecidos en el artículo 28.3 del RGPD (véase también el Artículo 3.3 de las BCR-C anteriores).

Por ejemplo, los Miembros de las BCR han elaborado e implementado una Política de Seguridad de la Información (Apéndice 10 de estas BCR-C). Localmente, los Miembros de las BCR también pueden haber implementado políticas de seguridad

más específicas. Al firmar un acuerdo con subcontratistas/Encargados, los Miembros de las BCR se reservan el derecho de evaluar el nivel de seguridad proporcionado por la parte contratante para el procesamiento de los Datos Personales.

4.8 Evaluación de Impacto en la Protección de Datos

La Evaluación de Impacto en la Protección de Datos (DPIA, por sus siglas en inglés) es un proceso basado en riesgos introducido por el Reglamento General de Protección de Datos (RGPD) que permite al Responsable de los datos describir el Procesamiento de Datos Personales, demostrar su necesidad y proporcionalidad, y ayudar a gestionar los riesgos para los derechos y libertades de las personas naturales resultantes del Procesamiento de Datos Personales, evaluándolos y determinando las medidas para abordarlos. Los miembros de las BCR se comprometen a realizar las DPIAs de acuerdo con el **Anexo 09 Procedimiento para la Evaluación de Impacto en la Protección de Datos.**

Cuando un tipo de Procesamiento, que implica en particular el uso de nuevas tecnologías, es probable que resulte en un alto Riesgo para los derechos y libertades de los Titulares de los datos, los miembros de las BCR, teniendo en cuenta la naturaleza, alcance, contexto y propósitos del procesamiento y antes de su realización, llevarán a cabo una DPIA. Este requisito también se aplicará a las operaciones de Procesamiento existentes cuando se prevea una modificación de la operación de procesamiento y dicha modificación pueda resultar en un alto Riesgo para los derechos y libertades de los Titulares de los datos.

El procesamiento requerirá una Evaluación de Impacto en la Protección de Datos si se cumplen dos o más de los siguientes criterios:

- El procesamiento de la información incluye la evaluación o puntuación sistemática de aspectos personales relacionados con personas naturales, incluyendo la elaboración de perfiles y predicciones;
- El procesamiento de la información se basa en el procesamiento automatizado que afecta significativamente a la persona natural;
- El procesamiento de la información se realiza sobre Información sensible o de naturaleza altamente personal;
- La información se procesa a gran escala;
- El procesamiento combina o coincide con dos o más operaciones de procesamiento de información;
- El procesamiento de la información incluye una monitorización sistemática de un área de acceso público;
- El procesamiento se realiza sobre la información de personas vulnerables o niños;
- El procesamiento de la información incluye el uso innovador o la aplicación de soluciones tecnológicas u organizativas;
- El procesamiento de la información se realiza para propósitos diferentes a aquellos para los cuales se recopilaron los datos;
- El procesamiento de la información impide que los Titulares de los datos ejerzan sus derechos o utilicen un servicio o contrato.

Además, los miembros de las BCR llevarán a cabo una DPIA para las operaciones de Procesamiento que requieran una DPIA de acuerdo con la decisión de la lista de

operaciones de procesamiento de información que requieran una DPIA del Órgano de Vigilancia correspondiente del EEE.

Cuando una DPIA indique que el Procesamiento resultase en un alto Riesgo en ausencia de medidas adoptadas por el Responsable de los datos para mitigar el riesgo y cuando una DPIA revele altos Riesgos residuales, el miembro de las BCR buscará la consulta previa del Órgano de Vigilancia del EEE antes de llevar a cabo dicho Procesamiento.

Por ejemplo, la gestión de solicitudes de licencia de los empleados no se considera un proceso que presente un alto riesgo para los derechos y libertades de los Titulares de los datos. No obstante, siempre que un miembro de las BCR identifique un procesamiento que cumpla con dos o más de los criterios mencionados anteriormente, se realizará una DPIA bajo la supervisión del Oficial de privacidad de datos (DPO por sus siglas en inglés) de acuerdo con el procedimiento descrito en el Anexo 9.

4.9 Subprocesamiento y Transferencias fuera del Grupo Concentrix

Los miembros de las BCR se comprometen a no Transferir ningún Dato Personal a Responsables de los datos y/o Encargados de los datos que no sean miembros de las BCR, a menos que dichos Responsables y/o Encargados de los datos proporcionen garantías suficientes y hayan implementado medidas técnicas y organizativas adecuadas, como las proporcionadas en las BCR-C, de manera que el Procesamiento cumpla con los requisitos de estas BCR-C.

En este sentido, los miembros de las BCR han implementado medidas técnicas, físicas y administrativas adecuadas para asegurar y controlar que los Datos Personales no sean accedidos y/o procesados ilegalmente.

Cualquier miembro de las BCR está obligado a celebrar un contrato escrito u otro acto jurídico vinculante con cualquier Responsable de los datos o Encargado de los datos fuera del Grupo Concentrix (o no vinculado por las BCR-C) si están Procesando Datos Personales. El mencionado contrato u otro acto jurídico vinculante deberá establecer los elementos mencionados en el Artículo 3.3. Dicho contrato puede incluir estas BCR-C.

Así, si un miembro de las BCR, actuando como Responsable de los datos o Encargado de los datos en nombre de otro miembro de las BCR, utiliza los servicios de un subcontratista establecido fuera del EEE y necesita, para el Propósito de los servicios prestados, compartir los Datos Personales de sus empleados (sólo en la medida necesaria para las operaciones), el miembro de las BCR evaluará, antes de la Transferencia, que el subcontratista sea capaz de cumplir con los requisitos de las BCR-C y asegurará la Transferencia mediante el acto jurídico vinculante adecuado.

4.9 Implementación de medidas de notificación en la violación de Datos personales

Cuando ocurra una Violación de Datos Personales, los miembros de las BCR deberán cumplir con el procedimiento aplicable de Violación de Datos adoptado por Concentrix.

En cualquier caso, los miembros de las BCR deberán, sin demora indebida y, cuando sea factible, a más tardar 72 horas después de haberse dado cuenta de la Violación de Datos Personales, notificar la Violación de Datos Personales a (1) Webhelp SAS (como el Miembro Responsable de las BCR) y a los otros Líderes Locales de Privacidad relevantes cuando dicho miembro de las BCR actúe como Responsable de los datos, así como al miembro de las BCR que actúe como Responsable de los datos cuando un miembro de las BCR que actúe como Encargado de los datos se dé cuenta de una Violación de Datos Personales (2) al Órgano de Vigilancia competente del EEE, a menos que la Violación de Datos Personales sea improbable que resulte en un riesgo para los derechos y libertades de las personas naturales.

La notificación mencionada deberá cubrir al menos la siguiente información:

- La Naturaleza de la Violación de Datos Personales y alcance de la Violación de Datos Personales, incluyendo cuando sea posible las categorías y el número aproximado de Titulares de los datos afectados y las categorías y el número aproximado de registros de Datos Personales afectados;
- Nombre y datos de contacto del Oficial de Privacidad del Grupo (**DPO** por sus siglas en inglés) u otro punto de contacto donde se pueda obtener más información;
- Descripción de las consecuencias que probablemente resulten de la Violación de Datos Personales;
- Descripción de las medidas tomadas o propuestas por el Responsable de los datos para abordar la Violación de Datos Personales, incluyendo, cuando sea apropiado, medidas para mitigar sus posibles efectos adversos.

Cualquier miembro de las BCR, cuando procese Datos Personales por su cuenta como Responsable de los datos, y cuando procese Datos Personales en nombre de otro miembro de las BCR que actúe como Responsable de los datos, también podrá necesitar comunicar a los Titulares de los datos sobre la Violación de Datos Personales cuando dicha Violación de Datos Personales sea probable que resulte en un alto riesgo para los derechos y libertades de las personas naturales de acuerdo con el Artículo 34 del RGPD. En tales circunstancias, la comunicación deberá realizarse sin demora indebida y cubrirá los elementos mencionados anteriormente que serían comunicados al Órgano de Vigilancia competente del EEE.

Los miembros de las BCR deberán documentar cualquier Violación de Datos Personales y la información mencionada anteriormente. A petición, los miembros de las BCR deberán poner esta documentación a disposición del Órgano de Vigilancia competente del EEE.

En caso de una violación de seguridad que conduzca a la destrucción, pérdida, alteración, divulgación no autorizada o acceso accidental o ilegal a los Datos Personales transmitidos, almacenados o de otro modo procesados, los miembros de las BCR procederán de acuerdo con el procedimiento de Violación de Datos Personales descrito en el **Anexo 08 Procedimiento para la Notificación de Violación de Datos Personales.**

5. Tratamiento de Datos Sensibles

Los Miembros de las BCR se comprometen a cumplir con las disposiciones del Artículo 4 – Principios para el Tratamiento de Datos Personales y reconocen que los Datos Personales Sensibles requieren la implementación de una protección específica, ya que dichos Datos Personales podrían crear riesgos significativos en relación con los derechos y libertades fundamentales del Titular de los datos.

Los Miembros de la BCR se comprometen a procesar Datos Personales Sensibles de acuerdo con la Legislación Aplicable de Protección de Datos y, cuando sea aplicable, con cualquier otro marco sectorial adoptado por el Órgano de Vigilancia del EEE.

Dicho Tratamiento deberá ser limitado y específico, en particular en relación con los empleados de Concentrix.

Cuando un Miembro de la BCR tenga la intención de procesar Datos Personales Sensibles en su propio nombre, asegurará que:

- El Tratamiento sea necesario y legal; o
- El Tratamiento se lleve a cabo con salvaguardas y controles adecuados; o
- Cuando sea necesario, el Titular de los Datos haya dado su consentimiento explícito para el Tratamiento de esos Datos Personales Sensibles para uno o más fines específicos. Dicho consentimiento no se considerará necesario cuando (1) el Titular de los Datos no esté en condiciones de dar su consentimiento y el Tratamiento es necesario para proteger los intereses vitales del Titular de los Datos o de otra persona; (2) el Titular de los Datos haya manifestado claramente que los Datos Personales Sensibles afectados son parte del dominio público; (3) Cuando sea aplicable, el Tratamiento está explícitamente permitido por la Legislación de Protección de Datos Aplicable o cualquier ley nacional (por ejemplo, registro/protección de minorías); o
- establecer, ejercer o defender reclamaciones legales, siempre que no haya motivos para suponer que el Titular de los datos tiene un interés legítimo primordial en garantizar que dichos datos no sean Procesados.
- Cuando sea necesario, el Tratamiento sea esencial para el establecimiento, ejercicio o defensa de reclamaciones legales, siempre que no haya motivos para suponer que el Titular de los Datos tiene un interés legítimo predominante en asegurar que dichos datos no sean procesados.

6. Transferencia de Datos Personales a países terceros y restricción de la Transferencia Ulterior a Miembros que no sean de las BCR

6.1 Transferencias y Transferencias Ulteriores de Datos Personales

En el transcurso de sus actividades, los Miembros de las BCR pueden Transferir Datos Personales a otras entidades del grupo Concentrix (que sean o no Miembros de las BCR) o a terceros. Dichas entidades de Concentrix y/o terceros pueden estar ubicados fuera del Espacio Económico Europeo (en adelante, “EEE”). En tal caso, se considera que se producen Transferencias de Datos Personales.

Cuando se transfieran Datos Personales, Concentrix implementará garantías específicas para asegurar que los Datos Personales transferidos cuenten con un nivel adecuado de protección, según se detalla a continuación:

- Las Transferencias de Datos Personales de un Miembro de la BCR, actuando como Responsable de los Datos, a otro Miembro de la BCR ubicado fuera del EEE y actuando como Responsable de los Datos o como Encargado de Datos, estarán respaldadas por las disposiciones de esta BCR-C; o
- Las Transferencias de Datos Personales de un Miembro de la BCR actuando como Responsable de los Datos a una entidad del grupo Concentrix (que no sea un Miembro de la BCR) o a terceros ubicados fuera del EEE (más específicamente, en un país fuera del EEE que haya recibido una decisión de adecuación por parte de la Comisión Europea) y que actúen como Encargado de Datos estarán respaldadas por un acuerdo escrito que incluya las cláusulas contractuales tipo aplicables adoptadas por el Órgano de Vigilancia Competente del EEE y/o la Comisión Europea, como las Cláusulas Contractuales Tipo de la Comisión Europea sobre Transferencias (914/2021), Módulo 2 Responsable a Encargado; o
- Las Transferencias de Datos Personales de un Miembro de la BCR actuando como Responsable de los Datos a una entidad de Concentrix (que no sea un Miembro de la BCR) o a terceros ubicados fuera del EEE (más específicamente, en un país fuera del EEE que haya recibido una decisión de adecuación por parte de la Comisión de la UE) y que actúen como Responsable de los Datos estarán respaldadas por un acuerdo escrito que incluya las cláusulas contractuales tipo aplicables adoptadas por el Órgano de Vigilancia Competente del EEE y/o la Comisión de la UE, como las Cláusulas Contractuales Tipo de la Comisión Europea sobre Transferencias (914/2021), Módulo 1 Responsable a Responsable.
- En ausencia de una decisión de adecuación o salvaguardas apropiadas como se describe anteriormente, las Transferencias pueden llevarse a cabo excepcionalmente si se aplica una derogación de acuerdo con el Artículo 49 del RGPD y deberán, cuando sea relevante, ser ocasionales y no repetitivas.

En cualquier caso, los Miembros de la BCR se comprometen a no transferir Datos Personales a terceros que no sean parte del grupo Concentrix (o a una entidad de Concentrix que no sea un Miembro de la BCR) sin asegurarse primero de que se garantice un nivel adecuado de protección en línea con el proporcionado por el RGPD, con el fin de asegurar que el nivel de protección de los Titulares de Datos garantizado bajo el RGPD no se vea comprometido.

Más específicamente, los Miembros de la BCR acuerdan que los Datos Personales que se hayan transferido bajo las BCR-C entre dos Miembros de la BCR solo pueden ser transferidos posteriormente fuera del EEE a Encargados de Datos y Responsables de Datos que no estén vinculados por las BCR-C, siempre que se cumplan los requisitos sobre Transferencias establecidos en los Artículos 44 a 46 del RGPD y reflejados en este documento.

6.2 Obligación del Importador de Datos en caso de solicitud de acceso por parte del gobierno

Sin que se vea afectada la obligación del Miembro de las BCR que actúe como Importador de Datos de informar al Exportador de Datos sobre su imposibilidad de cumplir con los compromisos contenidos en el BCR-C (Artículo 12.3 a continuación), el Miembro de las BCR que actúe como Importador de Datos notificará de inmediato al Exportador de Datos y, cuando sea posible, al Titular de Datos (si es necesario con la ayuda del Exportador de Datos) si:

- Recibe una solicitud legalmente vinculante de una autoridad pública bajo las leyes del país de destino, o de otro tercer país, para la divulgación de Datos Personales transferidos de conformidad con las BCR-C. Dicha notificación incluirá información sobre los Datos Personales solicitados, la autoridad solicitante, la base legal de la solicitud y la respuesta proporcionada;
- Se entera de cualquier acceso directo por parte de autoridades públicas a los Datos Personales transferidos de conformidad con al BCR-C de acuerdo con las leyes del país de destino. Dicha notificación incluirá toda la información disponible para el Importador de Datos.

Si se le prohíbe notificar al Exportador de Datos y/o al Titular de Datos, el Importador de Datos utilizará sus mejores esfuerzos para obtener una exención de dicha prohibición, con el fin de comunicar la mayor cantidad de información posible y lo antes posible, y documentará sus mejores esfuerzos para poder demostrarlos a solicitud del Exportador de Datos.

El Importador de Datos proporcionará al Miembro de las BCR que actúe como Exportador de Datos, a intervalos regulares, la mayor cantidad de información relevante posible sobre las solicitudes recibidas (en particular, número de solicitudes, tipo de datos solicitados, autoridad o autoridades solicitantes, si las solicitudes han sido impugnadas y el resultado de tales impugnaciones, etc.). Si el Importador de Datos está o se ve parcial o completamente prohibido de proporcionar al Exportador de Datos la información mencionada anteriormente, deberá informarlo al Exportador de Datos sin demora indebida.

El Importador de Datos conservará la información mencionada anteriormente durante el tiempo que los Datos Personales estén sujetos a las salvaguardas proporcionadas por las BCR-C, y la pondrá a disposición del Órgano de Vigilancia Competente si es solicitado.

El Importador de Datos revisará la legalidad de la solicitud de divulgación, en particular si se mantiene dentro de los poderes otorgados a la autoridad pública solicitante, y refutará la solicitud si, después de una evaluación cuidadosa, concluye que existen motivos razonables para considerar que la solicitud es ilegal según las leyes del país de destino, las obligaciones aplicables bajo el derecho internacional y los principios de cortesía internacional.

El Importador de Datos, bajo las mismas condiciones, buscará posibilidades de apelación.

Al impugnar una solicitud, el Importador de Datos buscará medidas provisionales con el fin de suspender los efectos de la solicitud hasta que la autoridad judicial competente haya decidido sobre el fondo del asunto. No divulgará los Datos Personales solicitados hasta que sea requerido para hacerlo según las normas procesales aplicables.

El Importador de Datos documentará su evaluación legal y cualquier impugnación a la solicitud de divulgación y, en la medida en que lo permitan las leyes del país de

destino, pondrá la documentación a disposición del Exportador de Datos. También la pondrá a disposición del Órgano de Vigilancia Competente si es solicitado.

El Importador de Datos proporcionará la mínima cantidad de información permitida al responder a una solicitud de divulgación, basada en una interpretación razonable de la solicitud.

En cualquier caso, las Transferencias de Datos Personales por un Miembro de las BCR a cualquier autoridad pública no pueden ser masivas, desproporcionadas e indiscriminadas de una manera que vaya más allá de lo necesario en una sociedad democrática (véase el Artículo 12.3 de las BCR-C al respecto)

7. Derechos de los Titulares de Datos

7.1. Derechos de Beneficiarios Terceros

Siempre que un Miembro de las BCR procese Datos Personales como Responsable del Tratamiento o como Encargado del Tratamiento en su nombre, **los Titulares de Datos tienen derecho a hacer cumplir esta BCR-C como beneficiarios terceros.**

Los Titulares de Datos deberán al menos poder hacer cumplir los siguientes elementos:

- Base legal para el tratamiento (Artículo 4.1);
- Limitación del propósito del Tratamiento (Artículo 4.2);
- Minimización de Datos (Artículo 4.3);
- Limitación de los períodos de almacenamiento (Artículo 4.6);
- Exactitud de los Datos (Artículo 4.5);
- Seguridad de los Datos Personales, especialmente:
    - Protección de datos desde el diseño y por defecto y medidas para garantizar la seguridad de los datos (Artículos 12 y 4.7);
    - Notificación de Violación de Datos Personales cuando la violación de Datos Personales pueda resultar en un alto riesgo para sus derechos y libertades (Artículo 4.10).
- Reglas específicas para el tratamiento de categorías especiales de Datos Personales y Datos Personales relacionados con condenas penales y delitos (Artículo 5);
- Transparencia y fácil acceso a esta BCR-C (Artículo 12.1);
- Transferencias ulteriores (Artículo 4.9);
- Derechos de acceso, rectificación, eliminación, restricción, notificación respecto a la rectificación o eliminación o restricción a cada destinatario al que se hayan divulgado los Datos Personales, objeción al tratamiento, derecho a la portabilidad de datos, derecho a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado, incluyendo la elaboración de perfiles (Artículos 7.4 y 7.5);
- Legislación nacional que impida el cumplimiento de las BCR (Artículo 12.3) y en caso de solicitudes de acceso gubernamental (Artículo 6.2);
- Derecho a presentar una queja a través del mecanismo de quejas interno de las empresas (Artículo 8 de las BCR y Apéndice 5 – Artículo 3.1);
- Obligaciones de cooperación con el Órgano de Vigilancia del EEE (Artículo 12.4);

- Derecho a presentar una queja ante el Órgano de Vigilancia competente del EEE (elección ante el Órgano de Vigilancia en el Estado Miembro de su residencia habitual, lugar de trabajo o lugar de la supuesta infracción) y ante el tribunal competente del Estado Miembro de la UE (elección del Titular de Datos para actuar ante los tribunales donde el responsable o encargado tenga un establecimiento o donde el Titular de Datos tenga su residencia habitual) (Artículo 8);
- Deber de informar a los Titulares de Datos sobre cualquier actualización de las BCR-C y de la lista de Miembros de las BCR que estén vinculados por la presente BCR-C (Artículo 13);
- Los derechos de los actuales beneficiarios terceros (Artículo 7);
- Derecho a remedios judiciales y derecho a obtener reparación y, cuando corresponda, compensación en caso de incumplimiento de uno de los elementos exigibles de las BCR-C (Artículos 7 y 8 de los BCR, y Apéndice 5 – Artículo 3.4.2).

Por lo tanto, los Miembros de las BCR reconocen que los Titulares de Datos tienen derecho a buscar remedios judiciales y/o remedios ante una autoridad de protección de datos bajo las condiciones definidas a continuación, por cualquier incumplimiento de uno de los elementos exigibles de las BCR-C como se enumera arriba y a recibir compensación por cualquier daño resultante de la violación de las BCR-C por parte de cualquier Miembro de las BCR.

Un Miembro de las BCR acepta que los Titulares de Datos pueden ser representados por un organismo, organización o asociación sin fines de lucro para presentar la queja en su nombre y ejercer los derechos enumerados anteriormente. Dicho organismo, organización o asociación debe estar debidamente constituido de acuerdo con la legislación de un Estado Miembro, tener objetivos estatutarios de interés público y estar activo en el ámbito de la protección de los derechos y libertades de los Titulares de Datos en lo que respecta a la protección de sus Datos Personales.

Para mayor claridad, se especifica que los derechos de beneficiarios terceros descritos anteriormente no se extienden a aquellos elementos de las BCR-C relacionados con mecanismos internos implementados dentro de las entidades, como detalles de formación, programas de auditoría, redes de cumplimiento y mecanismos para la actualización de las BCR-C.

Tenga en cuenta que, sin perjuicio del presente Artículo 7, Concentrix anima a los Titulares de Datos a utilizar el mecanismo de quejas interno descrito en el Artículo 8 de las BCR-C que se proporciona a continuación.

7.2. Derecho a presentar una queja y obtener remedio judicial, reparación y compensación cuando un Miembro de las BCR dentro del EEE no cumpla con las BCR-C

Cuando un Miembro de las BCR dentro del EEE no cumpla con uno de los elementos exigibles de las BCR-C como se enumera en la sección 7.1 anterior, Concentrix reconoce que el Miembro de las BCR dentro del EEE responsable del

incumplimiento asumirá la responsabilidad y tomará las acciones necesarias para remediar sus actos.

Concentrix también reconoce que el Titular de Datos tendrá derecho a:

- Presentar una queja ante un Órgano de Vigilancia del EEE, en particular en el Estado Miembro de su residencia habitual, lugar de trabajo o lugar de la supuesta infracción; y/o;
- Un remedio judicial efectivo cuando afirme que esta BCR-C ha sido infringida por un Miembro de las BCR como Responsable del Tratamiento o por un Miembro de las BCR como Encargado del Tratamiento que procese Datos Personales en su nombre. Concentrix reconoce que dicho reclamo puede presentarse ante el tribunal competente del Estado Miembro donde esté establecido el Miembro de las BCR responsable del incumplimiento o ante el tribunal donde el Titular de Datos tenga su residencia habitual.

7.3 Derecho a presentar una queja y obtener remedio judicial, reparación y compensación cuando un Miembro de las BCR fuera del EEE no cumpla con las BCR-C

Cuando un Miembro de las BCR fuera del EEE no cumpla con uno de los elementos exigibles de las BCR-C enumerados anteriormente, Webhelp SAS como Entidad Europea Principal (1) acepta ser el “Miembro Responsable de las BCR” y, como tal, asume la responsabilidad por cualquier daño material e inmaterial resultante del incumplimiento del BCR-C, incluyendo el pago de compensación cuando sea otorgado por el tribunal competente, y (2) se compromete a tomar las acciones necesarias para remediar los actos de dicho otro Miembro de las BCR fuera del EEE.

En tales circunstancias, Webhelp SAS también reconoce que cualquier Titular de Datos que considere que el Miembro de las BCR ubicado fuera del EEE (actuando como Responsable del Tratamiento o Encargado del Tratamiento) ha infringido uno de los elementos exigibles enumerados en la Sección 7.1, tendrá derecho a:

- Presentar un reclamo ante una autoridad de protección de datos en el lugar donde resida, trabaje o donde el Miembro de las BCR con responsabilidad delegada esté establecido. Y/o;
- Un remedio judicial efectivo como si la violación hubiera sido causada por Webhelp SAS en lugar del Miembro de las BCR ubicado fuera del EEE, ante los tribunales o autoridades judiciales donde esté basado Webhelp SAS, o donde el Titular de Datos resida o trabaje.

Cuando los Titulares de Datos puedan demostrar que han sufrido daños y establecer hechos que muestren que es probable que el daño haya ocurrido debido a la infracción de las BCR-C, Webhelp SAS será responsable de demostrar que dicho Miembro de las BCR fuera del EEE no fue responsable de la infracción de las BCR-C que dio lugar a esos daños, o que no hubo tal infracción. En caso de que Webhelp SAS pueda demostrar que el otro Miembro de las BCR ubicado fuera del EEE no fue responsable del acto, también podrá eximirse de cualquier responsabilidad.

7.4 Derechos de los Titulares de Datos

Los Titulares de Datos tienen derecho a beneficiarse de los siguientes derechos:

- Acceder a los Datos Personales que le conciernen y que son Procesados por un Miembro de las BCR;
- Solicitar la rectificación o eliminación de cualquier Dato Personal inexacto o incompleto que le concierna, y de cualquier Dato Personal respecto al cual el propósito del Tratamiento ya no sea legal o apropiado;
- Solicitar que el Tratamiento de sus Datos Personales que le concierne sea limitado;
- Objetar al Tratamiento de sus Datos Personales por un Miembro de las BCR cuando dicho Tratamiento sea necesario para los fines de los intereses legítimos perseguidos por el Miembro de las BCR actuando como Responsable del Tratamiento o por un tercero, con fines de interés legítimos, incluyendo la elaboración de perfiles en cualquier momento, por motivos relacionados con su situación personal individual, a menos que los intereses perseguidos por el Miembro de las BCR prevalezcan sobre los intereses, derechos y libertades de los Titulares de Datos;
- Objetar al Tratamiento de sus Datos Personales para fines de marketing, incluida la elaboración de perfiles; y
- Recibir sus Datos Personales en un formato estructurado, de uso común, legible por máquina e interoperable cuando el Tratamiento se realice por medios automatizados.

Cuando un Miembro de las BCR actúe como Responsable, manejará dicha solicitud sin demora indebida y de acuerdo con el procedimiento de manejo de quejas especificado en la Sección 8 a continuación.

El Miembro de las BCR que actúe como Responsable deberá comunicar cualquier rectificación o eliminación de Datos Personales o restricción del Tratamiento realizada a raíz de una solicitud del Titular de Datos a cada destinatario al que se hayan divulgado los Datos Personales, a menos que esto resulte imposible o implique un esfuerzo desproporcionado. Además, dicho Miembro de las BCR deberá informar al Titular de Datos sobre esos destinatarios si el Titular de Datos lo solicita.

7.5 Ejercicio de los Derechos de los Titulares de Datos

Los Titulares de Datos tienen derecho a hacer cumplir esta BCR-C como beneficiarios terceros y a ejercer sus derechos respecto al Tratamiento de sus Datos Personales por cualquier Miembro de las BCR que actúe como Responsable del Tratamiento. El Miembro de las BCR deberá asegurarse de que cualquier solicitud o queja del Titular de Datos en relación con el ejercicio de sus derechos (“**Solicitudes**”) sea atendida de manera oportuna.

Los Titulares de Datos pueden hacer una solicitud verbal o por escrito. Los Miembros de las BCR proporcionarán a los Titulares de Datos medios accesibles para ejercer sus derechos y, en particular:

1 - Un único correo electrónico dedicado para ser utilizado independientemente del país en el que se encuentre un Titular de Datos: dpo@concentrix.com y protección.dedatos@concentrix.com

Los correos electrónicos locales pueden usarse para tener en cuenta las especificidades locales, como el idioma.

Para contactar a tu contacto local de privacidad, por favor, consulta el Apéndice 01 - Lista de entidades Concentrix vinculadas por las BCR-C y contactos locales de privacidad por correo electrónico.

2 - Portal único con dirección de correo electrónico del DPO accesible en www.concentrix.com

3 - Dirección postal única para ser utilizada independientemente del país en el que se encuentre un Titular de Datos:

Oficial de Privacidad de Datos del Grupo

Departamento Legal y de Cumplimiento

3 rue d'Heliopolis

75017 – PARIS

FRANCIA

El DPO, o cualquier otra persona o entidad, interna o externa, designada por el DPO para la gestión de las Solicitudes, deberá (i) asegurarse de haber obtenido la información mínima requerida del Titular de Datos correspondiente para atender su Solicitud y (ii), si se considera necesario, obtener la mayor cantidad de información posible para permitir que la Solicitud sea manejada adecuadamente.

Si existe una duda sobre la identidad de la persona que realiza la solicitud, especialmente al usar medios de comunicación a distancia, un Miembro de las BCR puede necesitar solicitar más información sobre el Titular de Datos. La información recopilada deberá ser (i) limitada a la necesaria para confirmar la identidad de la persona que hace la solicitud y (ii) no se deberá recopilar cuando los productos o servicios proporcionados por un Miembro de las BCR o sus Clientes no se entreguen bajo la identidad real del usuario. La proporcionalidad siempre deberá ser evaluada por el Responsable del Tratamiento.

En cualquier caso, la respuesta a un Titular de Datos deberá ocurrir dentro de un plazo máximo de 1 mes después de recibir la Solicitud. Teniendo en cuenta la complejidad y el número de las solicitudes, dicho plazo de un mes puede extenderse, como máximo, por dos meses adicionales, en cuyo caso el reclamante deberá ser informado en consecuencia (como se detalla en el Apéndice 5).

Cuando el Titular de Datos no esté satisfecho con la respuesta inicial proporcionada por el Miembro de las BCR, dicho Titular de Datos tendrá derecho, en cualquier caso, a solicitar inmediatamente que su Solicitud sea reexaminada. El Titular de Datos deberá proporcionar al Miembro de las BCR una explicación detallada de las disposiciones insatisfactorias de la solución proporcionada anteriormente. El Miembro de las BCR deberá tomar no más de 2 meses desde la recepción de la Solicitud de reexaminación para determinar cómo se manejará y deberá informar al Titular de Datos por escrito en consecuencia.

Si una Solicitud o queja del Titular de Datos es rechazada por el Miembro de las BCR o la respuesta no satisface al Titular de Datos, o en cualquier caso, el Titular de Datos puede contactar al DPO y/o presentar directamente una queja ante un Órgano de Vigilancia competente del EEE y/o buscar remedio judicial, como se detalla más arriba en las secciones 7.1 y 7.2.

Más detalles sobre este Artículo están disponibles en el siguiente apéndice:

- **Apéndice 5 - Procedimiento para las solicitudes de los Titulares de Datos donde Concentrix actúe como Responsable de los Datos**

8. Proceso para el manejo de denuncias de los Titulares de los Datos.

Los Titulares de los Datos tienen derecho a presentar una denuncia directamente con un Miembro de las BCR con respecto al Procesamiento de Datos que ellos consideren que no cumplan con las BCR-C ante el Miembro de las BCR que consideren que no cumple. Cuando sea probable que la violación ocurra por un acto de un Miembro de las BCR ubicado fuera del Espacio Económico Europeo (EEE), el Titular de los Datos puede presentar una denuncia directamente ante Webhelp SAS como la Entidad Europea Principal.

Los Titulares de los Datos pueden elevar una denuncia:

(1) Contactando por correo electrónico al Líder Local de Privacidad competente del Miembro de las BCR competente, en la dirección proporcionada en el Apéndice 01, y/o

(2) Contactando al Oficial del Grupo de Privacidad de los Datos al correo electrónico dpo@concentrix.com y protección.dedatos@concentrix.com , o por correo postal en la dirección ¾ rue d'Heliopolis, 75017, París, Francia. Dicha denuncia será manejada a su debido tiempo por el miembro competente de las BCR, con especial cuidado y atención, de acuerdo con los pasos y el tiempo definidos aquí. Tales cláusulas también son aplicables en relación con las solicitudes de los Titulares de los Datos para ejercer sus derechos (ver Artículo 7 anterior)

En la práctica, las denuncias interpuestas por los Titulares de los Datos serán manejadas de acuerdo con el procedimiento definido en el **Apéndice 5 – Procedimiento para las solicitudes de los Titulares de los Datos donde Concentrix actúa como Responsable de los Datos**.

El Miembro de las BCR que actúa como Responsable de los Datos debe informar al Titular de los Datos / demandante sobre las acciones tomadas sin demoras injustificadas, y en cualquier caso, dentro de un mes a partir de la fecha en la que fue presentada dicha denuncia, de acuerdo con las cláusulas aquí expuestas. La denuncia deberá ser manejada por un departamento o persona identificados claramente con un nivel adecuado de independencia en el ejercicio de sus funciones. En la práctica, el departamento o la persona competente debe ser el departamento Legal y de Cumplimiento Normativo (particularmente, el Oficial y/o el Líder Local de Privacidad). Teniendo en cuenta la complejidad y el número de solicitudes, ese plazo de un mes puede ser extendido a máximo dos meses adicionales, en cuyo caso el denunciante debe ser informado como corresponde.

En caso de que el miembro competente de las BCR decida rechazar una denuncia interpuesta por el Titular de los Datos, dicho miembro se compromete a informar al Titular de los Datos sobre su decisión y a entregarle información sobre la razón de tal rechazo.

En caso de que un Miembro de las BCR considere que una denuncia interpuesta por el Titular de los Datos es justificada, dicho Miembro de las BCR se compromete a implementar las medidas correctivas que considere adecuadas para remediar dicha situación tan pronto como sea razonablemente posible. Adicionalmente, el Miembro de las BCR también informará al Titular de la Información interesado una vez que las medidas correctivas hayan sido implementadas y la situación se haya solucionado.

En cualquier caso, los Miembros de las BCR reconocen que los Titulares de los Datos tienen derecho a presentar una petición ante un Órgano de Vigilancia del Espacio Económico Europeo (EEE) y/o buscar recursos judiciales. Los Miembros de las BCR también reconocen que dichos derechos no dependen de que los Titulares de los Datos hayan usado con antelación el proceso para el manejo de denuncias, sin embargo, se les incentiva a hacerlo.

9. Gobernanza de protección de datos

Concentrix definido una organización y gobernanza de la protección de Datos, la cual se define más a fondo en el Apéndice 3.

Los Miembros de las BCR se comprometen a designar un Oficial de Privacidad de Datos, donde se requiera y, en línea con el Artículo 37 RGPD, o cualquier otra persona o entidad (como el oficial encargado de la privacidad) con la responsabilidad de monitorear el complimiento de las BCR-C y goza del más alto apoyo administrativo para el cumplimiento de esta tarea. Esta organización es dirigida por el Oficial de Privacidad del Grupo, quien depende de una red de puntos de contacto de privacidad (específicamente los Líderes Regionales de Privacidad, Líderes Locales de Privacidad, además de los Referentes de Privacidad del Negocio) y quienes pueden ser designados como DPO por el miembro competente de las BCR.

El DPO nombrado formalmente con un Órgano de Vigilancia debe reportarse directamente con el nivel más alto de dirección. Adicionalmente, el DPO puede informar al nivel más alto de dirección si surge cualquier pregunta o problema durante el ejercicio de sus funciones.

El DPO no debe tener tareas que puedan dar lugar a conflictos de intereses. El DPO no debe encargarse de realizar evaluaciones del impacto de la protección de datos, y tampoco debe encargarse de realizar auditorías de las BCR si dicha situación resulta en un conflicto de intereses. Sin embargo, El DPO puede desempeñar un papel muy útil e importante al asistir a los Miembros de las BCR, y se deben pedir sugerencias del DPO.

Los roles y responsabilidades de la red, así como su gobernanza de trabajo son definidos en detalle en el **Apéndice 3 – Organización y gobernanza de la protección de datos.**

Adicionalmente, el DPO puede informar al nivel más alto de dirección si surgen preguntas o problemas durante el ejercicio de sus funciones.

El DPO y los Líderes Locales y Regionales de Privacidad pueden ser contactados a través de la información de contacto descrita en el Artículo 7.5 de las BCR-C y en los contactos de privacidad local suministrados en el Apéndice 01 de las BCR.

10. Entrenamiento y sensibilización

Proteger los Datos Personales no es sólo cuestión de cumplir con las leyes de privacidad, sino que hace parte de la materialización de los valores fundamentales de Concentrix. En este contexto, promover una cultura de la privacidad dentro del grupo es esencial para hacer que todos los empleados, aprendices, y otras personas cuyas conductas en el ejercicio de sus funciones estén bajo el control directo de los Miembros de las BCR, sean responsables de la protección de Datos Personales procesados como parte de sus operaciones.

Por lo tanto, estas BCR-C deben ser implementadas apropiadamente al interior de toda la organización. Para tal fin, los Miembros de las BCR han adoptado un programa de entrenamiento en privacidad, con el objetivo de asegurar que los empleados de Concentrix, aprendices, y otras personas cuya conducta, en el ejercicio de sus funciones estén bajo el control directo de los Miembros de las BCR, realmente están al tanto de las obligaciones, principios y procedimientos especificados en estas BCR-C. Además de los principios y obligaciones claves de la RGPD, el programa de entrenamiento y sensibilización debe cubrir, entre otros, procedimientos para manejar solicitudes de acceso a la información personal por parte de las autoridades públicas.

Dicho entrenamiento está dirigido a: (i) personas que tengan acceso permanente o regular los Datos Personales; (ii) personas involucradas en la recolección de Datos Personales; y/o (iii) personas involucradas en el desarrollo de herramientas utilizadas para procesar Datos Personales.

El material para el entrenamiento debe ser actualizado y revisado regularmente, al menos anualmente o luego de haber cambios significativos en la Legislación Aplicable de Protección de Datos, con el fin de asegurar que se reflejen en la última versión de las BCR-C.

El programa de entrenamiento apuntará a proporcionar:

- Un nivel básico de conocimiento fundamental de los principios que aplican al momento de Procesar los Datos Personales y un buen conocimiento de los procesos existentes y su implementación, y
- Entrenamiento específico adaptado a las diferentes funciones dentro de la organización.

En este sentido, se recuerda que los Miembros de las BCR reconocen que no se puede hacer ninguna transferencia bajo las BCR-C a otro Miembro de las BCR, a menos que este último sea vinculado efectivamente por las BCR-C y se pueda proporcionar un entrenamiento efectivo sobre las BCR-C a los empleados del respectivo Miembro de las BCR.

Los Miembros de las BCR se comprometen a asegurar que todos los empleados de Concentrix, sus aprendices y otras personas cuyas conductas, que en el ejercicio de

su trabajo estén bajo control directo de los Miembros de las BCR, tomen el entrenamiento una vez esté disponible y, posteriormente, completen el curso de actualización anual.

En el siguiente apéndice se encuentran más detalles con respecto a este artículo:

- **Apéndice 04 – Programa de entrenamiento y sensibilización.**

11. Privacidad por diseño / privacidad por defecto

Con el fin de asegurar que los principios definidos en esta BCR-C sean tomados en cuenta efectivamente y se reflejen en los diferentes Procesamientos que se llevan a cabo, Concentrix tomará en consideración la protección de datos e implementará medidas técnicas y organizacionales desde el inicio de cualquier proyecto nuevo.

Con el fin de proporcionar un alto nivel de protección a los Datos Personales dentro de la organización, los principios y obligaciones definidas en adelante serán integradas por consiguiente al diseño de cada proyecto de acuerdo con los procedimientos de privacidad por diseño adoptados por Concentrix.

12. Transparencia y Cooperación

1.1 Comunicación de las BCR-C

El Miembro de las BCR se compromete a asegurar que a todos los Titulares de los Datos se les proporcione información sobre sus derechos de beneficiarios terciarios, con respecto al procesamiento de sus Datos Personales, y sobre los medios para ejercer esos derechos. Dicha información se describe en el Artículo 7 de las BCR-C.

Concentrix comunicará abiertamente estas BCR-C a los Titulares de los Datos y las hará fácilmente accesible para cualquier persona. Dicha comunicación debe permitirle a cualquier Titular de los Datos obtener una copia de estas BCR-C sin demoras injustificadas y en un formato abierto. Adicionalmente, una versión pública de la última versión de las BCR-C actuales debe estar disponible en cualquier momento para los Titulares de los Datos en el sitio web de Concentrix www.concentrix.com. Los Titulares de los Datos también puede solicitar una copia de las BCR-C contactando al DPO en dpo@concentrix.com y privacidad.dedatos@concentrix.com.

La versión pública de las BCRs-C debe contener, al menos, la siguiente información:

- Una descripción del alcance de las BCR-C (Artículo 2 de las BCR-C),
- La cláusula relacionada con las responsabilidades del Grupo (Artículo 7 de las BCR-C),
- Las cláusulas relacionadas con los principios de protección de datos (Artículo 4, 4.1, 4.2, 4.3, 4.5, 4.6, 4.7, 4.9, 4.10 y 5 de las BCR-C),
- La licitud del procesamiento (Artículo 4.1 y 5 de las BCR-C),
- Notificaciones de seguridad y de violaciones a la información personal (Artículo 4.7 y 4.10 de las BCR-C)

- Restricciones en transferencias ulteriores (Artículo 4.9 y Artículo 6 de las BCR-C), y
- Las cláusulas relacionadas con los derechos de los Titulares de los Datos (Artículo 7, 8 y 12 de las BCR-C).

Esta información debe ser actualizada y presentada a los Titulares de los Datos de una manera clara, inteligible y transparente. Esta información debe ser proporcionada de manera completa, por consiguiente, un resumen de este documento no será suficiente.

La versión pública también debe incluir todas las políticas y procedimientos requeridos adjuntos a las BCR-C como Apéndice, especialmente para las BCR-C:

- Apéndice 01-A Lista de Miembros de las BCR vinculado por las BCR-C y los contactos de correos electrónicos de contacto de privacidad local
- Apéndice 02 Definiciones para los BCR y procedimientos
- Apéndice 05 Procedimiento para las solicitudes de los Titulares de los Datos donde Concentrix actúa como Responsable de los Datos.
- Apéndice 11-A Alcance material de las BCR-C: Lista de propósitos del procesamiento y las categorías relacionadas con los Datos Personales y los Titulares de los Datos.

Los otros Apéndices, o bien no son aplicables a las BCR-C, o bien son procesos internos irrelevantes para que los Titulares de los Datos entiendan o ejerzan sus derechos.

Estos requerimientos anteriores serán cumplidos al asegurar que la versión pública simplificada de las BCR-C, que contiene toda la información listada anteriormente, esté disponible en el sitio web de Concentrix (www.concentrix.com).

Concentrix promoverá el mejoramiento de la cultura de la privacidad y la seguridad dentro de su organización al compartir estas BCR-C a través de los sistemas y medios internos (por ejemplo, la Intranet de Concentrix, comunicaciones internas, etc.)

1.2 Información a los Titulares de los Datos

Los Miembros de las BCR, cuando actúen como Responsables de los datos, deben proporcionarle a los Titulares de los Datos cualquier información requerida por la Legislación Aplicable sobre Protección de Datos. Los Miembros de las BCR suministrarán dicha información sin demoras y dentro de un período de tiempo razonable después de obtener los Datos Personales, pero a más tardar en el plazo de un mes al momento de recibir la primera comunicación o divulgación con un destinatario legítimo. Tal información debe estar compuesta de, al menos, los siguientes elementos:

- La identidad y los detalles del contacto del Responsable de los Datos;
- Los detalles del contacto del Oficial de Privacidad de Datos (DPO) y/o del Líder de Privacidad;
- El propósito del Procesamiento y su base legal;
- Si la información no es recopilada directamente del Titular de los Datos, las categorías de los Datos Personales Procesados;
- El destinatario de los Datos Personales;
- Dado el caso que exista Transferencias de Datos fuera del EEE, los países a donde los Datos Personales sean transferidos, las medidas implementadas

para asegurar un nivel adecuado de protección y los medios por los cuales se obtiene una copia de ellos o dónde se han puesto a disposición;
- El período de retención de los datos;
- Los derechos de los Titulares de los Datos como se definen en el artículo 7 mencionado anteriormente. (por ejemplo, la existencia del derecho por parte del Responsable de los Datos a solicitar acceso y rectificación o eliminación de los Datos Personales, o restricción del Procesamiento con respecto al Titular de la Información, u objetar el procesamiento, así como también el derecho a la portabilidad de los datos);
- El derecho a presentar una denuncia ante un órgano de vigilancia;
- Cuando se recopilan los Datos Personales del Titular de la Información, si el Titular de la Información (1) está obligado a proporcionar los Datos Personales debido a cualquier requerimiento legal o contractual, o (2) tenga un requerimiento para proporcionar los Datos Personales ya que es necesario para celebrar un contrato, y las posibles consecuencias de no suministrar dichos datos.
- Si el procesamiento está basado en el consentimiento de los Titulares de los Datos, el derecho de ellos a retirar su consentimiento en cualquier momento sin afectar la licitud del Procesamiento basado en el consentimiento antes de su retiro.
- Si el procesamiento está basado en el interés legítimo de los Miembros de las BCR, las explicaciones de dicho interés legítimo.
- Según el caso, la existencia de toma de decisiones automatizadas, incluyendo el perfilamiento; y
- Cuando los Datos Personales no sean recopilados del Titular de la Información, cualquier información disponible en cuanto a sus fuentes (por ejemplo, en particular, las categorías de Datos Personales, fuente de la cual se originan los Datos Personales, la naturaleza pública de los Datos Personales);

Los Miembros de la BCR se comprometen a proporcionar dicha información a los Titulares de los Datos en un lenguaje accesible, fácil de entender, claro, simple y sencillo.

1.3 Inconsistencias con las legislaciones locales y prácticas que afectan el cumplimiento con las BCR-C

Los Miembros de las BCR se comprometen a usar las BCR-C como herramienta para las Transferencias sólo si se ha evaluado que la ley y las prácticas en un país tercero de destino – que no garantiza un nivel adecuado de protección aplicable al procesamiento de los Datos Personales por el Miembro de las BCR que actúa como Importador de los Datos, incluyendo cualquier requerimiento para revelar Datos Personales o medidas que autoricen el acceso por parte de las autoridades públicas – no impiden que este cumpla sus obligaciones bajo estas BCR-C.

Dicho compromiso se basa en el entendimiento de que las leyes y prácticas, que respetan la esencia de los derechos y libertades fundamentales, y no sobrepasan lo necesario y proporcional en una sociedad democrática para salvaguardar uno de los propósitos listados a continuación, no están en contradicción con las BCR-C:

(a) seguridad nacional, y/o,
(b) defensa, y/o,
(c) seguridad pública, y/o,
(d) la prevención, investigación, detección o procesamiento de delitos criminales o la ejecución de sanciones criminales, incluyendo la salvaguarda y prevención en contra de amenazas a la seguridad pública; y/o,
(e) otros objetivos importantes de interés público de la Unión o de un Estado Miembro, particularmente un interés económico o financiero de la Unión o de un Estado Miembro, incluyendo asuntos monetarios, presupuestales y tributarios, la salud pública y la seguridad social; y/o,
(f) La protección de la independencia judicial y de los procedimientos judiciales; y/o
(g) La prevención, investigación, detección y procesamiento de violaciones a la ética por profesiones reguladas; y/o
(h) un monitoreo, inspección o función regulatoria conectada, incluso de manera ocasional, con el ejercicio de la autoridad oficial en los casos referenciados en los puntos (a) hasta el (e); y/o
(i) la protección de los derechos del Titular de los Datos y las libertades de los demás; y, o
(j) la aplicación de demandas civiles

En la evaluación de las leyes y prácticas del País Tercero No Adecuado que puedan afectar el respeto de los compromisos contenidos en las BCR-C, los Miembros de las BCR deben tener en cuenta, particularmente, los siguientes elementos:

- **Las circunstancias específicas de las transferencias** o grupo de transferencias, y cualquier Transferencia ulterior prevista dentro del mismo país tercero o a otro País Tercero No Adecuado, incluyendo:
  - los propósitos por los cuales los Datos Personales son transferidos y Procesados (por ejemplo, mercadeo, RR.HH, almacenamiento, soporte de TI, pruebas clínicas);
  - tipos de entidades involucradas en el Procesamiento (el Importador de Datos y cualquier receptor de cualquier Transferencia ulterior)
  - el sector económico en el cual ocurre la Transferencia o grupo de Transferencias;
  - las categorías y el formato de los Datos Personales Transferidos;
  - ubicación del procesamiento, incluyendo el almacenamiento; y
  - canales de transmisión utilizados.
- **Las leyes y practicas del país tercero de destino**, relevantes a la luz de las circunstancias de la transferencia, incluyendo aquellas que requieren revelar los datos a las autoridades públicas o autorización al acceso por parte de dichas autoridades y aquellas que permitan acceder de estos Datos Personales durante el tránsito entre el país del Exportador de Datos y el país del importador de Datos, al igual que las limitaciones y salvaguardas aplicables.
- **Cualquier salvaguarda contractual, técnica u organizacional relevante** implementada para complementar las custodias bajo las BCR-C, incluyendo las medidas aplicadas durante la transmisión y al Procesamiento de los Datos Personales en el país de destino.

Donde se deban establecer salvaguardas adicionales a las previstas en las BCR-C, Concentrix, como Miembro Responsable de las BCR, el DPO y el **Líder Local de Privacidad** correspondiente serán informados e involucrados en dicha evaluación.

Los Miembros de las BCR deben documentar adecuadamente dicha evaluación, así como las medidas complementarias seleccionadas e implementadas. Dicha documentación se pondrá a disposición del Órgano de Vigilancia competente y al DPO cuando así la soliciten.

Adicionalmente, el Miembro de la BCR que actúa como Importador de los Datos debe notificar inmediatamente al Exportador de los Datos si, al hacer uso de estas BCR-C como una herramienta para las Transferencias, y por la duración de la membresía de la BCR, tiene razones creer que está o ha estado sujeto a leyes o prácticas que podrían impedir que cumpla sus obligaciones bajo las BCR-C, incluyendo los cambios posteriores de las leyes del País Tercero No Adecuado o una medida (como una solicitud de divulgación). Esta información también debe ser proporcionada al Miembro Responsable de las BCR y al DPO.

Tras la verificación de dicha notificación, el miembro de las BCR que actúa como Exportador de los Datos, junto con el Miembro Responsable de las BCR, y con la asistencia del DPO, del Líder Local de Privacidad competente y del equipo de Seguridad de la Información, deben comprometerse a identificar inmediatamente las medidas complementarias (como las medidas técnicas u organizacionales para asegurar la seguridad y la confidencialidad) que debe adoptar el Miembro de la BCR que actúa como Exportador de los Datos y/o Importador de los Datos, con el fin de permitirles cumplir sus obligaciones bajo las BCR-C. Lo mismo aplica si un Miembro de las BCR que actúa como Exportador de los Datos tiene razones para creer que un Miembro de la BCR, actuando como Importador de los Datos, ya no puede cumplir sus obligaciones en virtud de estas BCR-C.

Cuando el Miembro de las BCR que actúa como Exportador de los Datos (junto con el Miembro Responsable de las BCR y el DPO y/o el Líder Local de Privacidad competente) evalúe que las BCR-C, incluso si se acompañan de medidas complementarias, no pueden ser cumplidas por una Transferencia o un grupo de Transferencias, o si así lo indica el Órgano de Vigilancia competente, dicho miembro de las BCR se compromete a suspender la Transferencia o grupo de Transferencias en riesgo, así como todas las transferencias para las cuales la misma evaluación y razonamiento llevarían a un resultado similar, hasta que el cumplimiento sea asegurado nuevamente o la Transferencia sea terminada.

Tras dicha suspención, el Miembro de las BCR que actúa como Exportador de los Datos tiene que terminar la Transferencia o grupo de Transferencias si no se pueden cumplir las BCR-C, y no se restaura el cumplimiento de las BCR en el plazo de un mes a partir de la suspensión. En este caso, los Datos Personales que hayan sido transferidos antes de la suspensión, y cualquier copia de estos, deberán, a elección del Miembro de las BCR que actúa como Exportador de los Datos, ser regresados a este o deben destruirse en su totalidad.

Concentrix, como el Miembro Responsable de las BCR, y el DPO y/o el Líder Local de Privacidad competente, informarán a todos los demás Miembros de las BCR sobre la evaluación realizada y sus resultados, de modo que las medidas complementarias identificadas sean aplicadas, en caso de que el mismo tipo de Transferencias sea llevado a cabo por cualquier otro miembro de las BCR o, cuando no se puedan implementar las medidas complementarias efectivas, las transferencias en cuestión se suspenden o se finalizan.

El Miembro de las BCR que actúa como Exportadores de los Datos debe monitorear – de manera continua y, cuando lo considere apropiado, en colaboración con los Importadores de los Datos – los desarrollos en Países Terceros No Adecuados a los cuales los Exportadores de los Datos han transferido Datos Personales que podrían afectar la evaluación inicial del nivel de protección y las decisiones tomadas en consecuencia sobre dichas Transferencias.

1.4 El deber de cooperar

En cualquier caso, los Miembros de las BCR acuerdan cooperar con los Órganos de Vigilancia del EEE, incluso aceptando ser auditados o inspeccionados (en sede o de forma remota) por dichos Órganos de Vigilancia, para tener en cuenta las recomendaciones, y acatar la decisión del Órgano de Vigilancia competente del EEE que se pueda aportar con relación a estas BCR-C. Los Miembros de las BCR reconocen y están de acuerdo en que los poderes y derechos de auditoría del Órgano de Vigilancia competente no pueden limitarse, particularmente en relación con auditoría práctica llevada a cabo por dicho Órgano de Vigilancia.

Los Miembros de la BCR y, cuando corresponda, sus respectivos representantes deben poner a disposición del Órgano de Vigilancia del EEE, al ser solicitada, cualquier información sobre las operaciones de procesamiento cubiertas por las BCR-C, tales como los registros de las actividades de procesamiento.

Cualquier conflicto relacionado con el ejercicio de supervisión del cumplimiento de las BCR-C por parte del Órgano de Vigilancia competente será resuelto en los tribunales del Estado Miembro de dicho Órgano de Vigilancia, de acuerdo con las leyes procedimentales de ese Estado Miembro. Los Miembros de las BCR acuerdan someterse a la jurisdicción de estas cortes.

13. Programa de auditoría que abarca las BCR

Cada Miembro de las BCR que actúe como Responsable debe encargarse de, y ser capaz de demostrar, el cumplimiento con las BCR-C. Para ello, y adicionalmente a los requisitos establecidos en el artículo **4.4 (Posesión de un Registro)**, 4.8 (Evaluación del Impacto de la Protección de Datos) y los Apéndices 08 – Notificación de violaciones a los Datos Personales, los Miembros de la BCR deben cumplir con los siguientes requerimientos sobre el programa de auditoría de la protección de datos.

El Miembro de las BCR se compromete a desarrollar e integrar en su programa de auditoría la revisión de su complimiento con las BCR-C. El programa de auditoría permitirá definir:

- una frecuencia razonable de acuerdo a la cual se deben llevar a cabo las auditorías;
- el alcance esperado de la auditoría; y
- el equipo a cargo de la auditoría.

El proceso de auditoria se detalla en el **Apéndice 7 – Procedimientos para las Auditorías de Privacidad de los Datos**. La auditoría cubre todos los aspectos de esta BCR-C (por ejemplo, aplicaciones, sistemas de TI, bases de datos que procesan

los datos personales, o transferencias ulteriores, decisiones tomadas con respecto a los requisitos obligatorios bajo las leyes nacionales que entran en conflicto con las BCR-C, la revisión de los términos contractuales utilizados para las transferencias fuera del Grupo a los responsables y a los encargados de los datos, las medidas correctivas, etc.) incluyendo los métodos y planes de acción que aseguren que se llevarán a cabo las medidas correctivas. Sin embargo, no es necesario que dicho programa de auditoría, necesariamente, monitoree todos los aspectos de las BCR-C que cada miembro está auditando, siempre y cuando se monitoreen todos los aspectos de las BCR-C a intervalos regulares apropiados para ese Miembro de las BCR.

Los miembros de las BCR se comprometen a hacer que las auditorías se lleven a cabo con frecuencia (al menos anualmente y/o si hay indicadores de incumplimiento) para asegurar la verificación del cumplimiento con las BCR-C o considerando el nivel de riesgo de una actividad de Procesamiento cubierta por las presentes BCR-C para los derechos y libertades de los Titulares de los Datos.

Adicionalmente a las auditorías regulares, las auditorías específicas (auditorías ad hoc) pueden ser solicitadas por el DPO y/o el miembro de la red de privacidad competente (por ejemplo, el Líder Local de Privacidad), o cualquier otra función competente en el grupo Concentrix, tal como el departamento de auditoría interna. Dichas auditorías pueden ser llevadas a cabo por auditores acreditados internos o externos recomendados por el DPO y/o el miembro competente de la red de privacidad. El mapa de ruta es iniciado y terminado por el DPO y/o el miembro competente de la red de privacidad, como se especifica en el Apéndice 7. En cualquier caso, los auditores externos deben ser independientes y estar sujetos a una obligación legal de confidencialidad y/o estar bajo a una obligación legal de confidencialidad adecuada.

El DPO es responsable de determinar el alcance de las auditorías a realizarse. Para tal propósito, éste puede consultar al Comité de Privacidad y/o encargarle al equipo de auditorías internas de Concentrix que determine el alcance de dicha auditoría. La auditoría puede ser realizada por el DPO del Grupo y/o los miembros competentes de la red de privacidad (por ejemplo, el Líder Local de Privacidad) y/o por el equipo de auditoría interna de grupo Concentrix, o cualquier otra función relevante dentro de Concentrix siempre que:

- se les garantice independencia a las personas a cargo para desempeñar sus funciones en estas auditorías; y
- las personas encargadas de auditar el cumplimiento con las BCR-C, si dicha situación genera un conflicto de intereses.

Los resultados de cada auditoría deben ser presentados al DPO del Grupo y/o a los miembros de la red de privacidad (como los Líderes Locales de Privacidad) y/o al Comité de Privacidad y/o a los miembros de la junta directiva de Concentrix. El reporte final, la identificación de defectos y las acciones correctivas deben ser compartidas y aplicadas por el Líder Local de Privacidad. Con base en la evaluación del Líder Local de Privacidad, el reporte también puede ser compartido, cuando corresponda, con cualquier Referente de Privacidad del Negocio, gerente de seguridad local, propietarios del sistema/proceso, la junta directiva de la empresa matriz del grupo Concentrix o la junta directiva del Miembro de las BCR competente sujeto a la auditoría o cualquier otro empleado interno requerido. Las

acciones correctivas serán definidas con un orden de prioridad para determinar un cronograma de implementación de dichas medidas.

Concentrix reconoce que los Órganos de Vigilancia competentes del EEE pueden solicitar la comunicación de los resultados de la auditoría y, por consiguiente, acuerda concederles acceso a ellos una vez se soliciten. Los resultados de los reportes de auditoría y los reportes de auditorías internas relevantes se conservarán de forma que los Órganos de Vigilancia ubicados en el EEE puedan tener acceso a ellos si ejercen su derecho de auditoría establecido a continuación.

Los Miembros de las BCR se comprometen a asegurar que los Órganos de Vigilancia Competentes puedan tener acceso a los resultados de la auditoría una vez se soliciten, y no deben limitar dichos derechos, especialmente por motivos de confidencialidad, por ejemplo, relacionados con la protección de secretos del negocio.

Se recuerda que los Miembros de las BCR deben autorizar a cualquier Órgano de Vigilancia competente del EEE a que ellos mismos realicen auditorías de protección de datos sobre cualquier cuestión relacionada con las BCR-C. En este sentido, cada miembro de las BCR debe permitir que el Órgano de Vigilancia del EEE audite al Miembro de las BCR pertinente para que el Órgano de Vigilancia del EEE pueda obtener la información necesaria para demostrar que el (los) Miembro(s) cumple(n) con estas BCR-C (ver también el Artículo 12.4 mencionado anteriormente).

14. Cambios a las BCR-C

El DPO de Concentrix, con el apoyo de los Líderes Locales de Privacidad, se asegurarán de que las presentes BCR-C se mantengan actualizadas (por ejemplo, teniendo en cuenta las modificaciones del ambiente regulatorio, las recomendaciones de las autoridades de protección de datos de la UE, o cambios en el alcance de las BCR-C).

Particularmente, el DPO debe mantener una lista actualizada con las entidades vinculadas por las BCR-C. Cuando cualquier entidad nueva de Concentrix resulte vinculada de manera efectiva por las BCR-C (como se especifica en el Artículo 3.2), el DPO debe actualizar la lista y debe informar sin demora injustificada a todos los Miembros de las BCR y a los Órganos de Vigilancia pertinente del EEE a través del Órgano de Vigilancia competente del EEE. Dicha información actualizada será puesta a disposición de los Titulares de los Datos junto con las BCR-C a través de los mismos medios.

Webhelp SAS reportará dichos cambios al Órgano de Vigilancia del EEE al menos una vez al año o cuando el DPO lo considere necesario. La notificación de dichos cambios a los Órganos de Vigilancia del EEE se realizarán al menos una vez al año a través del Órgano de Vigilancia competente, con una breve explicación de las razones justificando la actualización. Los Órganos de Vigilancia también deberían ser notificados al menos una vez al año, siguiendo el mismo proceso, en caso de que no se haya hecho ningún cambio.

La notificación o actualización anual también deben incluir la renovación de la confirmación con respecto al hecho de que Concentrix, como el Miembro

Responsable de las BCR, haga los arreglos apropiados para permitirse el pago de la compensación por cualquier daño como resultado de una violación a las BCR-C por los Miembros de la BCR fuera del EEE.

En la misma medida, cuando una enmienda tenga un impacto substancial en las BCR-C o en el nivel de protección de los derechos concedidos por esta BCR-C, Concentrix, con la ayuda del DPO, se compromete a informar de inmediato a los Miembros de las BCR y a los Órganos de Vigilancia del EEE.

15. Incumplimiento con las BCR-C

Al constituirse como Miembro de las BCR, el Exportador de Datos y el Importador de Datos deben cumplir con los siguientes requisitos:

- No debe hacerse ninguna transferencia a un Miembro de las BCR a menos que el Miembro de las BCR esté vinculado de manera efectiva por las BCR-C y pueda dar cumplimiento
- El Importador de los Datos debe informar de inmediato al Exportador de los Datos si es incapaz de cumplir con las BCR-C, por cualquier razón, incluyendo las situaciones descritas detalladamente en el Artículo 12.3 de las BCR-C anteriormente mencionadas
- Cuando el Importador de los Datos viole las BCR-C o sea incapaz de cumplir con ellas, el Exportador de los Datos debe suspender la Transferencia (Ver también el artículo 12.3 de las BCR-C mencionadas anteriormente).
- El Importador de los Datos debe, a elección del Exportador de los Datos, regresar o borrar inmediatamente en su totalidad los Datos Personales que hayan sido Transferidos bajo las BCR-C, cuando:
- El Exportador de los Datos haya suspendido la transferencia, y el cumplimiento con estas BCR-C no sea restaurado en un plazo razonable, y en cualquier caso dentro de un plazo de un mes de suspensión; o
- El importador de los Datos se encuentre violando de manera considerable o persistente las BCR-C.
- El Importador de los Datos no cumpla con una decisión vinculante de una corte competente o de un Órgano de Vigilancia Competente con respecto a sus obligaciones bajo las BCR-C.

Los mismos compromisos deben aplicar a cualquier copia de los datos. El Importador de los Datos debe certificar la eliminación de los datos al Exportador de los Datos.

Hasta que los datos sean eliminados o regresados, el Importador de los Datos debe continuar asegurando el cumplimiento con las BCR-C.

En caso de que las leyes locales que aplican al Importador de Datos prohíban la devolución o eliminación de los Datos Personales transferidos, el Importador de los Datos debe garantizar que continuará asegurando el cumplimiento con las BCR-C, y sólo procesará los datos en la medida, y durante el tiempo que lo requiera la ley local.

Para los casos en que las leyes y/o prácticas locales aplicables afecten el cumplimiento con las BCR-C, ver el Artículo 12.3 de las BCR-C mencionadas anteriormente.

16. Terminación

Un Miembro de las BCR que actúe como importador de los Datos, que deje de estar vinculado por las BCR-C puede conservar, regresar, o eliminar los Datos Personales recibidos bajo las BCR-C.

Si el Exportador de los Datos está de acuerdo con que los datos sean guardados por el Importador de los Datos, se debe mantener la protección en línea con el Capítulo V GDPR y como se refleja en el Artículo 6 de las BCR-C.

17. Apéndices

- Apéndice 01 - Lista de Miembros de las BCR vinculados por las BCR-C y los correos electrónicos de contacto de privacidad local
- Apéndice 02 - Definiciones para los BCR y procedimientos
- Apéndice 03 – Gobernanza y organización de la Privacidad
- Apéndice 04 - Programa de concienciación y formación sobre privacidad.
- Apéndice 05 - Procedimiento para las solicitudes de los Titulares de Datos cuando los Miembros de las BCR actúan como Responsables del Tratamiento
- Apéndice 06 - Procedimiento para las solicitudes de los Titulares de Datos cuando los Miembros de las BCR actúan como Encargados del Tratamiento
- Apéndice 07 – Procedimiento de Auditoría
- Apéndice 08 - Procedimiento en caso de Violación a los Datos Personales
- Apéndice 09 – Evaluación del Impacto de la Protección de Datos.
- Apéndice 10 – Política de Seguridad de la Información
- Apéndice 11-A Lista BCR-C de propósitos del Procesamiento y las categorías relacionadas con los Datos Personales y los Titulares de los Datos. (Alcance del Material)
- Apéndice 11-B Lista BCR-P de propósitos del Procesamiento y las categorías relacionadas con los Datos Personales y los Titulares de los Datos. (Alcance Material)
- Apendice 12 Contrato Marco de Tratamiento de Datos Personales.

CONTROL DE DOCUMENTO

Versión	Actualización	Resumen de modificaciones
0.1	27/02/2022	Aprobación Final
0.2	01/01/2023	Actualización de la lista de Miembros de las BCR
0.3	24/02/2023	Actualización de la lista de Miembros de las BCR
0.4	01/04/2024	Rebranding y formateado Alineación con recomendaciones EDPB 1/2022 derogación y sustitución WP256_Rev01

Frecuencia de Revisión	Este documento será revisado al menos anualmente o en caso de cambios
Fecha de emisión	25/05/2018
Dominio	Privacidad
Clasificación	Público
Referencia	EN__GPPriv-01- Binding Corporate Rules - Controller

Normas corporativas vinculantes en calidad de Encargado

Nuestras BCRs para el Encargado se aplican únicamente a la filial de Concentrix bajo Concentrix, que actúa como Entidad Europea Principal.

Las filiales a las que se aplican las BCR se enumeran en el Apéndice 01 de las BCR.

concentrix

Contenido

18. Introducción

Recordatorio: Tras la transacción entre Webhelp y Concentrix en septiembre del 2023, el nombre comercial del grupo es ahora Concentrix. Sin embargo, es importante tener en cuenta que el alcance de las presentes BCR no se ha modificado. Las BCR sólo son aplicables a las Afiliadas de Concentrix que actúen como Entidad Principal Europea. Las afiliadas que están sujetas a las BCR (Responsable y/o Encargado) se enumeran en el Apéndice 01 y se las denominará Miembros de las BCR.

En el Grupo Concentrix, creemos que la protección de los Datos Personales no es sólo una cuestión de seguridad o cumplimiento de un marco legal particular, sino un compromiso individual y organizacional. La divulgación y el intercambio de los estándares de Concentrix a través de las Normas Corporativas Vinculantes para Encargados (en adelante, las "BCR-P") y las presentes Normas Corporativas Vinculantes para Responsables (en adelante, las "BCR-C") es de suma importancia en relación con las expectativas legítimas de los Titulares de los Datos sobre cómo se Procesan sus Datos Personales.

En el curso de sus actividades, los Miembros de las BCR procesan tanto Datos Personales internos como de Clientes. En este sentido, los Miembros de las BCR protegen los Datos Personales que procesan en su nombre mediante la implementación de medidas y controles técnicos, físicos y administrativos adecuados, incluidos en las presentes BCR-P. Dichos controles garantizarán que toda la organización Procese los Datos Personales de manera consistente, independientemente de la naturaleza y/o el lugar del Procesamiento.

Este enfoque es particularmente importante debido a la diversidad de actividades que Concentrix cubre en nombre de sus Clientes.

Como consecuencia de lo anterior y teniendo en cuenta los requisitos introducidos por el Reglamento Europeo 2016/679 adoptado el 27 de abril de 2016 (en adelante, el "Reglamento de la UE" o "RGPD") y las normas, reglamentos y leyes aplicables en el ámbito de la protección de datos, siempre que no contravengan el Reglamento de la UE, los Miembros de las BCR Procesarán los Datos Personales de acuerdo con los siguientes principios:

- **Licitud** – Los Datos Personales deben ser recolectados y procesados con el consentimiento del Titular de los Datos o cuando el Procesamiento sea legítimo o necesario de acuerdo con la Legislación Aplicable en Protección de Datos;
- **Lealtad** – El Procesamiento de Datos Personales debe tener en cuenta las circunstancias específicas y el contexto en el que se procesan dichos Datos Personales;
- **Transparencia** – La información y comunicación relacionadas con el Tratamiento de Datos Personales deben ser fácilmente accesibles, fáciles de entender, claras y en un lenguaje sencillo y claro;
- **Limitación de la finalidad** – Los Datos Personales deberán ser recolectados para fines específicos, explícitos y legítimos y no deben ser procesados de una manera que sea incompatible con dichos fines;

- **Minimización de datos** – Los Datos Personales recolectados deben ser adecuados, relevantes y limitados a lo necesario en relación con los fines para los que se procesan;
- **Exactitud** – Los Datos Personales deben ser exactos y, cuando sea necesario, se mantendrán actualizados. Se deben tomar todas las medidas razonables para asegurar que los Datos Personales inexactos, teniendo en cuenta los fines para los cuales se procesan, sean eliminados o rectificados sin demora indebida;
- **Limitación del almacenamiento** – Los Datos Personales deben mantenerse en una forma que permita la identificación de los Titulares de los Datos por no más tiempo del necesario para los fines que se procesan o cualquier otra retención legal;
- **Integridad y confidencialidad** – Los Datos Personales deben ser procesados de manera que garantice una seguridad adecuada, incluyendo protección contra el procesamiento no autorizado o ilegal y contra la pérdida, destrucción o daño accidental, utilizando medidas técnicas, físicas y administrativas apropiadas.

A través de estas BCR-P, Concentrix tiene la intención de compartir y especificar los detalles y los principios aplicables a todos los Miembros de las BCR y proporcionar ciertos estándares para todo el grupo que permitan la implementación de las BCR-P. Además, Concentrix podrá poner a disposición políticas específicas, locales o sectoriales. En caso de contradicción entre estas BCR-P y dichas políticas específicas, locales o sectoriales, prevalecerán los términos de las BCR-P, a menos que las disposiciones contradictorias de dichas políticas específicas, locales o sectoriales protejan mejor los derechos y libertades del Titular de los Datos.

Dado que las BCR-P tienen como objetivo garantizar un enfoque adecuado y consistente en toda la organización de Concentrix respecto al Procesamiento de Datos Personales, las excepciones que podrían resultar de legislaciones aplicables no se reflejan en estas BCR-P. Sin embargo, estas BCR-P incluyen un mecanismo de notificación en el Artículo 13.3, donde la legislación nacional impide que un Miembro de las BCR cumpla con las BCR-P y donde los Estados Miembros de la UE proporcionan reglas específicas adicionales al Reglamento de la UE. En consecuencia, la legislación local se considerará como una excepción aplicable a estas BCR-P y se registrará en consecuencia, tras la notificación correspondiente. Como se especifica en el Artículo 13.3, cuando esta legislación nacional imponga un nivel de protección más alto para los Datos Personales, dicha legislación nacional prevalecerá sobre las BCR-P.

19. Alcance

19.1 Alcance del Material

Esta BCR-P es aplicable siempre que un Miembro de las BCR Procese Datos Personales como Encargado de los datos.

Debido a la diversa gama de actividades que cubre Concentrix y al hecho de que procesa principalmente Datos Personales en nombre de sus Clientes, Concentrix puede tener que procesar varias categorías en constante evolución de Datos Personales, tales como:

- Información relacionada con la vida personal (por ejemplo, monitoreo de satisfacción del cliente, gestión de interacciones sociales en línea);
- Información económica y financiera (gestión de relaciones con clientes, prevención y detección de fraudes, facturación, informes y análisis
- Información de identificación (por ejemplo, gestión de llamadas entrantes y salientes, gestión de operaciones de exclusión, marcación y enrutamiento de interacciones, escucha y grabación de interacciones);
- Información técnica (por ejemplo, marcación y enrutamiento de interacciones, análisis para operaciones entrantes y salientes, solución de análisis de voz); o

El alcance del material se detalla con mayor precisión en el **Anexo 11-B**, que proporciona una tabla detallada sobre el Propósito del Procesamiento y las categorías relacionadas de Titulares de Datos y de Datos Personales cubiertas por la presente BCR-P.

No obstante lo anterior, esta BCR-P se aplica al Procesamiento de Datos Personales por parte de los Miembros de las BCR que actúan como Encargado del Tratamiento, independientemente de la categoría y naturaleza de dichos Datos Personales.

Los Miembros de las BCR también son los Responsables de los Datos Personales de sus empleados como su empleador. Al procesar Datos Personales de los empleados de Concentrix, los Miembros de las BCR cumplirán con las BCR-C y procesarán los Datos Personales según se describe en la Política de Privacidad de Empleados.

19.2 Alcance Geográfico

Concentrix desea implementar, en la medida de lo posible, un enfoque coherente dentro de la organización donde se procese Datos Personales. En consecuencia, todos los Miembros de las BCR, independientemente de su ubicación o jurisdicción legal, están sujetos a esta BCR-P. Como principio, no se llevará a cabo ninguna transferencia de Datos Personales por parte de ningún Miembro de las BCR a menos que esté vinculado por esta BCR-P a una entidad Concentrix que no esté vinculada por esta BCR-P. Cualquier transferencia de este tipo no puede llevarse a cabo a menos que dicha entidad Concentrix haya proporcionado garantías suficientes para implementar medidas técnicas y organizativas apropiadas de manera que el Procesamiento y las obligaciones asociadas a dicho Procesamiento cumplan con los requisitos de esta BCR-P y aseguren la protección de los derechos de los Titulares de los Datos. La entidad Concentrix vinculada por las BCR-P y la

entidad Concentrix no vinculada celebrarán un acuerdo escrito para garantizar esto.

20. Naturaleza Vinculante

20.1 Sobre los empleados de Concentrix

Dado que la protección de los Datos Personales es una cuestión de compromiso individual y organizacional, cada empleado debe cumplir con los requisitos especificados en esta BCR-P.

En consecuencia, las BCR-P forma parte del conjunto de políticas con las que los empleados de Concentrix están obligados a cumplir como parte de su contrato de trabajo. El incumplimiento de los principios y normas de esta BCR-P puede dar lugar a medidas disciplinarias que podrían resultar en la terminación del empleo y, en ciertos casos, en cargos criminales.

20.2 Sobre los Miembros de las BCR del grupo Concentrix

Como grupo, Concentrix quiere asegurar que todos los Miembros de las BCR pertenecientes a él estén obligados de la misma manera o de manera similar a los principios y obligaciones especificados en esta BCR-P y cumplan con los requisitos establecidos en la misma.

Por esta razón, esta BCR-P es vinculante para todos los Miembros de las BCR mediante la firma de un Acuerdo de Transferencia de Datos Intragrupo que incluye esta BCR-P como un apéndice.

La lista de entidades de Concentrix vinculadas por esta BCR-P se detalla en el Apéndice 1 de este BCR-P. Concentrix como Entidad Europea, con la asistencia del DPO, se compromete a mantener esta lista actualizada y disponible, y a comunicarla a solicitud de las partes relevantes según se determine de vez en cuando.

20.3 Dirigido a los Encargados de Datos de Concentrix

Cuando actúe en nombre de su Cliente como Encargado del Tratamiento, los Miembros de las BCR se comprometen a cumplir con esta BCR-P y a implementar los requisitos de la misma en relación con sus Clientes y los Titulares de los Datos de los Clientes. Cuando los Miembros de las BCR procesen los Datos Personales de los Titulares de Datos de sus Clientes, los Miembros de las BCR, así como cada empleado de los Miembros de las BCR involucrado en el Procesamiento, se comprometen a garantizar, de acuerdo con las instrucciones de los Clientes, la protección de los derechos de dichos Titulares de Datos y a proporcionar un nivel adecuado de protección a los Datos Personales que procesan, sujeto a lo dispuesto en la Sección 7 – Derechos de los Titulares de los Datos.

Cualquier actividad de Procesamiento llevada a cabo por un Miembro de las BCR en nombre de un Cliente deberá estar regida por un contrato escrito u otro acto jurídico vinculante, y deberá establecer (todos los elementos del artículo 28 del RGPD y, en particular, el objeto y la duración del Procesamiento, la naturaleza y el propósito del Procesamiento, el tipo de Datos Personales y las categorías de Titulares de los Datos, así como las obligaciones y derechos del Responsable de Datos. Además, este contrato u otro acto jurídico vinculante con un Encargado del Tratamiento deberá establecer las siguientes disposiciones:

1. Concentrix deberá mantener los Datos Personales confidenciales, especialmente asegurando que las personas autorizadas para Procesar Datos Personales se hayan comprometido a la confidencialidad o estén sujetas a una obligación legal de confidencialidad.
2. Concentrix deberá tomar medidas de seguridad técnicas, físicas y organizativas apropiadas para garantizar un nivel adecuado de seguridad para proteger los Datos Personales.
3. Concentrix no permitirá que el Sub-Encargado procese Datos Personales en relación con su obligación hacia el Cliente sin la autorización previa por escrito de este último, y garantizará que el Sub-Encargado se comprometa a cumplir con las mismas obligaciones que se establecen en el acto vinculante celebrado entre Concentrix y el Cliente a través de un contrato u otro acto legal bajo la legislación de la Unión o de los Estados Miembros. Cuando el Sub-Encargado no cumpla con sus obligaciones de protección de datos, el Encargado de Datos inicial seguirá siendo totalmente responsable ante el Miembro de las BCR por el cumplimiento de las obligaciones de ese otro Encargado de Datos.
4. Concentrix deberá poner a disposición del Cliente toda la información necesaria para demostrar su cumplimiento y contribuir a auditorías e inspecciones por parte del Cliente u otra autoridad relevante.
5. Concentrix deberá informar de manera inmediata al Cliente sobre cualquier violación de seguridad real o sospechada que involucre Datos Personales y apoyar al Cliente en la notificación al Órgano de Vigilancia relevante y en la comunicación a los Sujetos de Datos afectados, según sea el caso.
6. Concentrix deberá proporcionar toda la asistencia razonable al Cliente para llevar a cabo una evaluación de impacto sobre la protección de datos.
7. Concentrix deberá proporcionar todo el apoyo necesario al Cliente en relación con el manejo de solicitudes de los Titulares de Datos relacionadas con sus derechos.
8. Concentrix deberá cumplir con las instrucciones del Cliente respecto a la eliminación o devolución de los Datos Personales al finalizar el contrato u otro acto legal vinculante.
9. Concentrix deberá informar inmediatamente al Cliente si, en su opinión, una instrucción infringe esta BCR-P o la Legislación Aplicable en Protección de Datos.

Dicho contrato incluirá esta BCR-P para divulgar y hacer cumplir las Normas Corporativas Vinculantes ante ambas partes; los Clientes tienen derecho a hacer cumplir cualquier disposición de esta BCR-P contra un Miembro de las BCR o cualquier Miembro de las BCR con responsabilidad delegada. El contrato Estándar de Protección de Datos de Concentrix está ubicado en el anexo 12, el cual será

aceptado por parte de los contratistas y/o proveedores de Concentrix cuando procesen datos personales pertenecientes a los empleados y/o contratistas de Concentrix o actúe como sub-encargado.

21. Principios para el procesamiento de datos personales

Cuando actúen en nombre de sus Clientes como Encargado de Datos, los Miembros de las BCR deberán cumplir con los principios definidos a continuación. En cualquier caso, el Cliente será responsable de todo el Procesamiento de Datos Personales, independientemente del origen de los Datos Personales, realizado de acuerdo con la Legislación Aplicable en Protección de Datos y el Acuerdo de Servicio entre Concentrix y el Cliente.

21.1 Transparencia, equidad y licitud

Cuando actúe como Encargado de Datos, los Miembros de las BCR se comprometen a (1) proporcionar garantías suficientes e implementar medidas técnicas y organizativas apropiadas de manera que el Procesamiento cumpla con los requisitos de esta BCR-P, y (2) cooperar con el Responsable de los Datos, dentro de un tiempo razonable y en la medida razonablemente posible, y asistir al Cliente para cumplir con la Legislación Aplicable en Protección de Datos. Como Responsable de los Datos, el Cliente de los Miembros de las BCR sigue siendo responsable de garantizar que el Procesamiento que solicita a Concentrix cumpla efectivamente con la Legislación Aplicable en Protección de Datos.

Teniendo en cuenta la naturaleza del procesamiento y la información disponible, los Miembros de las BCR, a través de la finalización del Apéndice de Normas de Procesamiento de Datos, deberán asistir al Cliente cuando este crea que se requiere una evaluación de impacto sobre la protección de datos, basándose en la naturaleza, alcance, contexto y fines del procesamiento. En la medida en que el Cliente necesite asistencia adicional para llevar a cabo una evaluación de impacto sobre la protección de datos, para responder a investigaciones y consultas de las autoridades de protección de datos o para solicitar una consulta previa al Órgano de Vigilancia, los Miembros de las BCR, teniendo en cuenta la naturaleza del Procesamiento y la información disponible para ellos, proporcionarán asistencia al Cliente a través del Programa de Auditoría del Responsable de los Datos.

Además, los Miembros de las BCR deberán asegurarse de que los Datos Personales del Cliente almacenados en los sistemas de producción sean procesados por Concentrix de acuerdo con el artículo 28.3 (g) del Reglamento de la UE, tras la terminación del Acuerdo de Servicios. A menos que alguna Legislación Aplicable en Protección de Datos o cualquier otro Acuerdo de Servicios requiera el almacenamiento de los Datos Personales y sujeto a la solicitud escrita del Responsable de los Datos, los Datos Personales almacenados en los sistemas de producción deberán, a elección del Responsable, ser eliminados o devueltos tras la terminación del Acuerdo de Servicios. Los Miembros de las BCR deberán, dentro del plazo acordado con el Responsable, garantizar la confidencialidad de los Datos Personales transferidos por el Cliente y que los Miembros de las BCR no procesarán activamente los Datos Personales transferidos. El Responsable de los Datos reconoce que esta eliminación o restitución de Datos Personales (i) se limitará estrictamente a los Datos Personales proporcionados por el Responsable y

almacenados por Concentrix, actuando como Encargado, en el momento de la solicitud y (ii) tomará en cuenta los requisitos de almacenamiento de copias de seguridad y las políticas y estándares de seguridad.

Además, cuando un Miembro de las BCR tenga razones para creer que la legislación aplicable impide a este Miembro cumplir con sus obligaciones bajo esta BCR-P o tiene un efecto sustancial en las garantías proporcionadas por las BCR-P, este Miembro informará de inmediato al DPO, Concentrix y al otro Líder de Privacidad Local relevante, así como a los Clientes, según lo establecido en el Artículo **Erreur ! Source du renvoi introuvable.** (excepto cuando esté prohibido por la legislación local aplicable o por una autoridad de cumplimiento de la ley, como una prohibición bajo la ley penal para preservar la confidencialidad de una investigación de aplicación de la ley). En tal caso, el Cliente tiene derecho a suspender la transferencia o las actividades de Procesamiento en curso y / o a rescindir el contrato.

21.2 Limitación de propósito

Concentrix se compromete a cumplir con el principio general de limitación de la finalidad según el cual solo procesará los Datos Personales en nombre de su Cliente y en estricta conformidad con sus instrucciones documentadas cuando actúe como Encargado de Datos. Los Miembros de las BCR deberán informar de inmediato al Cliente si, en su opinión, una instrucción infringe la Legislación Aplicable en Protección de Datos.

Más concretamente, los Miembros de las BCR se comprometen a procesar los Datos Personales en nombre de su Cliente:

- para los únicos fines expresados por dicho Cliente;
- bajo las condiciones acordadas entre Concentrix y su Cliente en virtud del Acuerdo de Servicios; y
- por no más tiempo del que esté expresamente prescrito por el Cliente del Miembro de las BCR.

En caso de que un Miembro de las BCR no pueda garantizar dicho cumplimiento, se compromete a informar de inmediato a su Cliente, al DPO y al Líder de Privacidad Local relevante sobre su incapacidad para cumplir. Tal información del Miembro de las BCR a su Cliente deberá proporcionarse sin demora y tan pronto como el Miembro de las BCR tenga conocimiento de que dicho cumplimiento no es alcanzable. En tal caso, el Cliente tendría derecho a suspender la transferencia de Datos Personales al Miembro de las BCR o las actividades de Procesamiento en curso y / o a rescindir el contrato.

21.3 Calidad de los Datos

Los Miembros de las BCR se comprometen a ayudar y asistir al Cliente para cumplir con la Legislación Aplicable en Protección de Datos.

En particular, los Miembros de las BCR asistirán a sus Clientes para permitir que los Titulares de Datos ejerzan sus derechos mediante la ejecución de las medidas

necesarias solicitadas por sus Clientes para actualizar, corregir o eliminar los Datos Personales, o cualquier otro derecho que el Titular de Datos pueda hacer ejercer.

En tal caso, el Miembro de las BCR informará a cada Miembro de las BCR relevante (o Afiliado Concentrix no sujeto a las BCR) a quien se hayan divulgado los Datos Personales sobre cualquier corrección, eliminación o anonimización de los datos personales.

A solicitud de sus Clientes y cuando sea factible, los Miembros de las BCR también implementarán medidas para eliminar o anonimizar los Datos Personales en el momento en que la forma identificable de dichos datos ya no sea necesaria.

21.4 Registro de actividades de procesamiento

Cuando actúe como Encargado, los Miembros de las BCR deberán mantener un registro de todas las categorías de actividades de Procesamiento de Datos Personales realizadas en nombre de un Responsable de Datos, que debe mencionar al menos:

1. El nombre y los datos de contacto de los Miembros de las BCR y del/los Responsable(s) de Datos en nombre de los cuales actúa Concentrix;
2. Las categorías de procesamiento realizadas;
3. Las posibles transferencias de Datos Personales a un país tercero o a una organización internacional;
4. Una descripción general de las medidas de seguridad técnicas y organizativas para garantizar un nivel de seguridad adecuado al riesgo del procesamiento.

21.5 Seguridad

Donde actúen como Encargado de los Datos, los Miembros de las BCR se comprometen a cumplir con todas las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado a los riesgos presentados por el Tratamiento, cumpliendo al menos con los requisitos de la Legislación Aplicable en Protección de Datos, y en particular con el artículo 32 del RGPD y cualquier medida particular existente especificada en el Acuerdo de Servicio con el Cliente.

Los Miembros de las BCR deberán notificar al Cliente sin demora indebida después de enterarse de una violación de Datos Personales y deberán cumplir con el procedimiento aplicable de Violación de Datos Personales adoptado por los Miembros de las BCR en cooperación con el Responsable de los Datos.

21.6 Derechos de los Titulares de Datos

Los Miembros de las BCR se comprometen a ejecutar las medidas necesarias solicitadas por el Cliente y a comunicar cualquier información útil para ayudar a dicho Cliente a cumplir con su obligación de observar los derechos de los Titulares de Datos, según se detalla en la Sección 7 de esta BCR-P.

Teniendo en cuenta la naturaleza del tratamiento y la información disponible para el Encargado, los Miembros de las BCR proporcionarán asistencia y cooperación al Cliente, en la medida de lo posible y acordado con el Cliente, para el cumplimiento de la obligación del Cliente de responder a las solicitudes. Los Miembros de las BCR seguirán el Procedimiento para las solicitudes de los Titulares de Datos cuando actúen como Encargado de los Datos, anexado a esta BCR-P.

Cuando un Miembro de las BCR reciba una solicitud del Titular de los Datos para ejercer sus derechos, dicho miembro de las BCR informará al cliente y este último responderá a la solicitud. Según la Legislación Aplicable sobre Protección de Datos, el Cliente es responsable de gestionar la solicitud. El miembro de las BCR solo será responsable de seguir las Instrucciones adicionales de su Cliente sobre cómo gestionar dicha solicitud y de cooperar con el Cliente para gestionar estas solicitudes.

21.7 Subtratamiento y transferencias ulteriores

Los Miembros de las BCR o proveedores terceros pueden Subprocesar los Datos Personales de acuerdo con las disposiciones del Acuerdo de Servicio acordado con el Sliente. Los Subencargados deberán proporcionar garantías suficientes para implementar las medidas técnicas y organizativas adecuadas de manera que el Tratamiento de Datos cumpla con los requisitos de la Legislación Aplicable sobre Protección de Datos, estas BCR-P y cualquier acuerdo de Tratamiento de Datos aplicable.

Los Miembros de las BCR no utilizarán un Subencargado sin tener primero una autorización por escrito del Responsable. Al otorgar una autorización general para utilizar Subencargados, el Miembro de las BCR correspondiente informará al Cliente de cualquier cambio previsto en relación con la adición o sustitución de cualquier Subencargado y dará al cliente la oportunidad de refutar dichos cambios y de rescindir el formulario(s) de pedido aplicable(s) según se describe a continuación y en el Acuerdo de Servicio y el Acuerdo de Tratamiento de Datos. Siempre que los términos del Acuerdo de Servicio aplicable y del Acuerdo de Tratamiento de Datos y/o formulario(s) de pedido no priven al Responsable de los Datos del derecho a oponerse o a rescindir los servicios, el Responsable de los Datos podrá, mediante notificación por escrito al Miembro de las BCR correspondiente, rescindir el formulario(s) de pedido aplicable(s) en relación con aquellos Servicios que no puedan ser prestados por el Miembro de las BCR sin el uso del nuevo Subencargado objetado.

El Subencargado estará obligado por medio de un contrato u otro acto legal que requiera que dicho Subencargado cumpla con términos y obligaciones al menos tan estrictos y que ofrezcan al menos el mismo nivel de protección que los descritos en la Legislación de Protección de Datos, en estas BCR-P y en un Acuerdo de Tratamiento de Datos. El cliente podrá exigir razonablemente que el Miembro de las BCR comunique la lista de Subencargados autorizados para Procesar Datos Personales. El contrato deberá especificar los propósitos del Tratamiento, su naturaleza, las categorías de Datos Personales Procesados y las categorías de Titulares de Datos.

En caso de una obligación legal de divulgar Datos Personales a las autoridades competentes, los Miembros de las BCR involucrados deben notificar a Concentrix y al DPO. Concentrix se compromete a notificar al Órgano de Vigilancia del EEE relevante y, a menos que esté prohibido de otro modo, al Cliente sobre esta divulgación sin demora indebida y a cumplir con el principio de minimización de Datos. El Miembro de las BCR deberá precisar qué Sujetos de Datos están afectados por la divulgación, qué autoridad está solicitando esta divulgación y en qué base legal se fundamenta. En cualquier caso, los Miembros de las BCR se comprometen a no transferir Datos Personales a las autoridades públicas de manera masiva y desproporcionada. En ese mismo caso, los Miembros de las BCR se comprometen a notificar al Cliente sobre la divulgación. Cualquier notificación a un Miembro de las BCR y la notificación planificada a los Órganos de Vigilancia del EEE están sujetas al mecanismo y las disposiciones del Artículo 13.3 a continuación.

Además, cada Miembro de las BCR deberá garantizar y verificar que todos sus Subencargados y, en particular, cualquier otro Miembro de las BCR involucrado en el Tratamiento de Datos Personales, hayan sido debidamente aprobados por el Cliente, ya sea mediante una autorización general o específica por escrito.

5. Tratamiento de datos sensibles

Los Miembros de las BCR se comprometen a cumplir con las disposiciones del Artículo 4 – Principios para el Tratamiento de Datos Personales y reconocen que los Datos Personales Sensibles requieren la implementación de una protección específica, ya que dichos Datos Personales podrían crear riesgos significativos en relación con los derechos y libertades fundamentales del Titular de los datos.

Cuando los Miembros de las BCR sean requeridos por su Cliente para Procesar Datos Personales Sensibles, los Miembros de las BCR pueden ser requeridos para implementar medidas y controles de seguridad técnicos, físicos y administrativos adicionales.

Será responsabilidad del Cliente de los Miembros de las BCR definir qué medidas deben implementarse en este aspecto y asegurar que se cumplan los requisitos de la Legislación Aplicable sobre Protección de Datos y, cuando corresponda, de cualquier otro marco sectorial aplicable adoptado por los Órganos de Vigilancia del EEE.

Para mayor claridad, cuando se Procesen Datos Personales Sensibles como Encargados de Datos, los Miembros de las BCR no serán en ningún caso responsables de garantizar que el Tratamiento se base en una de las bases legales definidas en el Artículo 4 mencionado anteriormente – Principios para el Tratamiento de Datos Personales.

6. Transferencia de Datos Personales a países terceros y restricción de la Transferencia ulterior a Miembros que no sean de las BCR

6.1 Transferencias y Transferencias Ulteriores de Datos Personales

En el transcurso de sus actividades, los Miembros de las BCR pueden procesar Datos Personales en nombre de su(s) Cliente(s). Dichos Miembros de las BCR o Cliente(s) pueden estar ubicados fuera del Espacio Económico Europeo (en adelante, "EEE"), y por lo tanto, implicar Transferencias de Datos Personales. En tal caso, estas BCR-P se aplican a:

- Datos Personales recibidos de un Cliente que actúa como Responsable de los Datos y ubicado dentro del EEE, que luego son procesados por los Miembros de las BCR, actuando como Encargados del Tratamiento en nombre de este Cliente; y

- Transferencias de Datos Personales de un Miembro de las BCR actuando como Encargado del Tratamiento en nombre de un Cliente y ubicado dentro del EEE a otro Miembro de las BCR fuera del EEE, actuando como Encargado de datos.

De lo contrario, cuando se transfieran Datos Personales, Concentrix implementará garantías específicas para asegurar que los Datos Personales transferidos cuenten con un nivel adecuado de protección, como se detalla a continuación:

- Transferencias de Datos Personales desde un Miembro de las BCR que actúe como Encargado de Datos a un Afiliado de Concentrix (no sujeto a las BCR-P) o a terceros ubicados fuera del EEE (más específicamente en un país no perteneciente al EEE que haya recibido una decisión de adecuación por parte de la Comisión de la UE) y que actúe como Encargado de los Datos serán respaldadas por un acuerdo escrito que incluya las cláusulas Contractuales tipo aplicables adoptadas por el Órgano de Vigilancia competente del EEE y/o la Comisión de la UE (como las SCCs de la Comisión de la UE sobre Transferencias (914/2021), Módulo 3 Encargado a Encargado) siempre que el Encargado de los Datos haya permitido a Concentrix proceder con dicha transferencia en su nombre, incluyendo cualquier transferencia ulterior; o;
- Traspasos de Datos Personales desde un Miembro de las BCR que actúe como Encargado de los Datos a un Afiliado de Concentrix (no sujeto a las BCR-P) o a terceros ubicados fuera del EEE (más específicamente en un país no perteneciente al EEE que haya recibido una decisión de adecuación por parte de la Comisión de la UE) como Encargado de los Datos serán respaldados por un acuerdo escrito que incluya las cláusulas contractuales tipo aplicables adoptadas por el Órgano de Vigilancia competente del EEE y/o la Comisión de la UE (como las SCCs de la Comisión de la UE sobre Traspasos (914/2021), Módulo 4 Encargado a Responsable) siempre que el Responsable de los Datos haya permitido a

Concentrix proceder con dicho transferencia en su nombre, incluyendo cualquier transferencia ulterior.

- A falta de una decisión de adecuación o de salvaguardas apropiadas como se describe anteriormente, los Transferencias pueden realizarse excepcionalmente si se aplica una excepción conforme al Artículo 49 del RGPD y deberán ser ocasionales y no repetitivas.

En cualquier caso, los Miembros de las BCR que actúen como Encargado de los Datos se comprometen a no Transferir Datos Personales a terceros que no formen parte del Grupo Concentrix sin asegurarse primero de que se otorgará un nivel adecuado de protección en línea proporcionado por el RGPD a los Datos Personales transferidos, de modo que el nivel de protección del titular de los Datos sea garantizado bajo el RGPD y no se vea comprometido.

Para mayor claridad, cuando un Miembro de las BCR actúe como Encargado de los Datos, solo procederá con la Transferencia bajo instrucciones documentadas del Responsable de los Datos, a menos que esté obligado a hacerlo por la legislación de la Unión o del Estado Miembro a la que esté sujeto dicho Miembro de las BCR. En tal caso, el Miembro de las BCR deberá informar al Responsable de los Datos sobre dicho requerimiento legal antes de Procesar los Datos Personales, a menos que dicha ley prohíba tal información por razones importantes de interés público reconocidas en la legislación de la Unión o en la legislación del Estado Miembro a la que esté sujeto el Responsable de los Datos.

6.2 Obligación del Importador de los Datos en caso de solicitud de acceso por parte del gobierno

Sin que se vea afectada de la obligación del Miembro de las BCR que actúe como Importador de los Datos de informar al Exportador de los Datos sobre su incapacidad para cumplir con los compromisos contenidos en las BCR-P (Artículo 13.3 a continuación), el Miembro de las BCR que actúe como Importador de los Datos notificará de inmediato al Exportador de los Datos y, cuando sea posible, al Titular de los Datos (si es necesario, con la ayuda del Exportador de los Datos) si:

- Recibe una solicitud legalmente vinculante de una autoridad bajo las leyes del país de destino, o de otro tercer país, para la divulgación de Datos Personales transferidos de conformidad con las BCR-P. Dicha notificación incluirá información sobre los Datos Personales solicitados, la autoridad solicitante, la base legal de la solicitud y la respuesta proporcionada;
- Tome conocimiento de cualquier acceso directo por parte de autoridades a los Datos Personales transferidos de conformidad con las BCR-P, de acuerdo con las leyes del país de destino. Dicha notificación incluirá toda la información disponible para el Importador de los Datos.

Si se le prohíbe notificar al Exportador de los Datos y/o al titular de los datos, el Importador de los Datos hará todo lo posible para obtener una exención de dicha prohibición, con el fin de comunicar la mayor cantidad de información posible y lo antes posible, y documentará sus mejores esfuerzos para poder demostrarlos a solicitud del Exportador de los Datos.

El Importador de los Datos proporcionará al Miembro de las BCR que actúe como Exportador de los Datos, a intervalos regulares, la mayor cantidad de información relevante posible sobre las solicitudes recibidas (en particular, el número de solicitudes, el tipo de datos solicitados, la autoridad o las autoridades solicitantes, si las solicitudes han sido impugnadas y el resultado de dichas impugnaciones, etc.). Si al Importador de los Datos se le prohíbe parcial o totalmente proporcionar al Exportador de los Datos la información mencionada anteriormente, lo informará al Exportador de los Datos sin demora indebida.

El Importador de los Datos conservará la información mencionada anteriormente mientras los Datos Personales estén sujetos a los Salvaguardas proporcionadas por las BCR-P, y la pondrá a disposición del Órgano de Vigilancia Competente a solicitud de esta.

El Importador de los Datos revisará la legalidad de la solicitud de divulgación, en particular, si se mantiene dentro de las facultades otorgadas a la autoridad solicitante, e impugnará la solicitud, si después de una evaluación minuciosa, concluye que existen razones fundamentadas para considerar que la solicitud es ilegal según las leyes del país de destino, las obligaciones aplicables bajo el derecho internacional y los principios de cortesía internacional.

El Importador de los Datos, bajo las mismas condiciones, buscará las posibilidades de apelación.

Al impugnar una solicitud, el Importador de los Datos buscará medidas cautelares con el fin de suspender los efectos de la solicitud hasta que la autoridad judicial competente se haya pronunciado sobre el fondo del asunto. No divulgará los Datos Personales solicitados hasta que esté obligado a hacerlo conforme a las normas procesales aplicables.

El Importador de los Datos documentará su evaluación legal y cualquier impugnación a la solicitud de divulgación y, en la medida en que lo permitan las leyes del país de destino, pondrá la documentación a disposición del Exportador de los Datos. También la pondrá a disposición del Órgano de Vigilancia Competente a solicitud de esta.

El Importador de los Datos proporcionará la mínima cantidad de información permitida al responder a una solicitud de divulgación, basada en una interpretación razonable de la solicitud.

En cualquier caso, los Traspasos de Datos Personales por un Miembro de las BCR a cualquier autoridad pública no pueden ser masivos, desproporcionados e indiscriminados de manera que superen lo necesario en una sociedad democrática (ver Artículo 12.3 de las BCR-P al respecto).

7. Derechos del Titular de los datos

7.1 Derechos de Beneficiario de Terceros

Cuando un Miembro de las BCR actúe como Encargado de los Datos en nombre de sus Clientes, los Titulares de los Datos podrán ejercer sus derechos respecto al Procesamiento de sus Datos Personales contra los Clientes Miembros de las BCR.

Sin embargo, cuando la solicitud de los Titulares de los Datos se refiera a requisitos impuestos a los Procesadores de Datos, los Titulares de los Datos deberán hacer cumplir al menos los siguientes derechos directamente contra los Miembros de las BCR:

- Deber de respetar las instrucciones del responsable de los Datos respecto al Procesamiento de Datos Personales, incluyendo para los Traspasos de Datos Personales a países terceros (Artículos 4.2 y 6).
- Deber de implementar medidas de seguridad técnicas y organizativas apropiadas y debe notificar cualquier Incidente de Violación de datos personales al Responsable de los Datos (Artículos 4.5, 4.7 y 3).
- Deber de cumplir con las condiciones al contratar a un Sub-Encargado que los Miembros de las BCR establezcan (Artículo 4.7).
- Deber de cooperar y asistir al Responsable de los Datos en el cumplimiento y la demostración de cumplimiento de la ley, como en la respuesta a solicitudes de los Titulares de los Datos en relación con sus derechos (Artículos 4.6 y 4.7).
- Acceso fácil a las BCR-P en el sitio web de Concentrix (actualmente en www.concentrix.com);
- Derecho a presentar quejas a través de mecanismos internos de reclamación (Artículo 8);
- Deber de cooperar con el Órgano de Vigilancia del EEE (Artículo 13.4);
- Disposiciones sobre responsabilidad, compensación y jurisdicción (Artículo 9);
- Legislación nacional que impida el cumplimiento de las BCR-P (Artículos 4.1, 6.2 y 13.3);
- Deber de garantizar la exigibilidad de los derechos de beneficiarios terceros (Artículo 7).

En cualquier caso, los Titulares de los Datos:

- Tienen derecho a buscar recursos judiciales por cualquier incumplimiento de los derechos garantizados bajo estas BCR-P y/o la Legislación de Protección de Datos Aplicable (Artículo 9);
- Tienen derecho a obtener reparación y, cuando corresponda, a recibir compensación por daños (incluyendo perjuicio material, así como cualquier angustia) resultantes de la violación de las BCR-P por cualquier Miembro de las BCR (Artículo 9);
- Tienen derecho a presentar una queja ante el Órgano de Vigilancia del EEE o ante los tribunales competentes para el Cliente ubicado en el EEE (Artículos 7.1 y 7.2).

Sin perjuicio de otros recursos de Concentrix, cuando el Encargado de los Datos y el Responsable de los Datos involucrados en el mismo Procesamiento sean responsables por cualquier daño causado por dicho Procesamiento, Titular de los

Datos tendrá derecho a recibir una compensación por el daño total directamente del Miembro de las BCR que actúe como Encargado de los Datos.

En el caso de que se pueda evidenciar que el Cliente ha desaparecido o ya no existe legalmente o se ha vuelto insolvente y ninguna otra entidad ha asumido las obligaciones legales de recuperar las obligaciones del Cliente, los Titulares de los Datos tienen expresamente el derecho a ejercer los siguientes derechos y a presentar un reclamo directo contra el Miembro de las BCR que actúe como Encargado de los Datos y esté vinculado por un Acuerdo de Servicio con el Cliente:

- Obligación de cumplir los elementos ejecutables de las BCR-P (artículos 3.1 y 3.2)
- Deber de garantizar la exigibilidad de los derechos de terceros beneficiarios (artículo 7);
- La aprobación por parte de Concentrix de i) la responsabilidad de pagar indemnizaciones y de remediar cualquier incumplimiento de las BCR-P por parte de un Miembro de las BCR ubicado fuera del EEE que resulte en daños recuperables, así como ii) la responsabilidad de demostrar que el Miembro de las BCR relevante no es responsable de la supuesta violación de las BCR-P que ha resultado en los daños reclamados por el Titular de los Datos (Artículo 7.2)
- Acceso fácil al BCR-P en el sitio web de Concentrix (actualmente en www.concentrix.com);
- Derecho a presentar una queja a través del mecanismo interno de quejas de las empresas (Anexo 5 – Artículo 3.1);
- Deberes de cooperación con el Órgano de Vigilancia del EEE (Artículo 13.4);
- Deber de cooperar con el Responsable de- los Datos (Artículo 4.1);
- Deber de cumplir con los principios para el Tratamiento de Datos Personales establecidos en el Artículo 4;
- Poner a disposición y actualizar la lista de entidades sujetas al BCR (Anexo 1); y
- Legislación nacional que impide el cumplimiento de las BCR-P (Artículo 13.3);

Un Miembro de las BCR acepta que los Titulares de Datos pueden ser representados por una entidad, organización o asociación sin fines de lucro para presentar la queja en su nombre y ejercer los derechos enumerados anteriormente. Dicha entidad, organización o asociación deberá estar debidamente constituida por la ley de un Estado Miembro, tener objetivos estatutarios que estén en interés público y estar activa en la protección de los derechos y libertades de los Titulares de Datos en relación con la seguridad de sus Datos Personales.

En pro de la claridad, se especifica que los derechos de terceros beneficiarios anteriormente descritos no se extienden a aquellos elementos de las BCR-P sobre mecanismos internos implantados en las entidades, tales como detalles de formación, programa de auditoría, red de cumplimiento y mecanismo de actualización de las BCR-P.

Tenga en cuenta que, sin perjuicio de lo dispuesto en el presente artículo 7, Concentrix anima a los Ttitulares de la Información a utilizar el mecanismo interno de reclamao descrito en el artículo 8 de las BCR-C que figura a continuación.

7.2 Derecho a reclamar y obtener reparación judicial, compensación e indemnización cuando un miembro de las BCR fuera del EEE no cumpla con el BCR-P

7.3 En caso de que un miembro de las BCR fuera del EEE no cumpla con las BCR-P, Concentrix (1) asume la responsabilidad de cualquier daño resultante del incumplimiento de las BCR-P, incluido el pago de una indemnización cuando la conceda el tribunal competente y (2) se compromete a tomar las medidas necesarias para remediar los actos de dicho otro miembro de las BCR.

En tales circunstancias, Concentrix también reconoce que el Titular de los datos tendrá derecho a:

- presentar una denuncia ante un Órgano de Vigilancia del lugar donde tenga su domicilio, lugar de trabajo o donde esté establecido el Miembro de las BCR con responsabilidad delegada; y/o;
- un recurso judicial efectivo cuando el Titular de los Datos considere que el Tratamiento de Datos Personales que le conciernen llevado a cabo por cualquier Miembro de las BCR que actúe como Encargado del Tratamiento infringe la presente BCR-P. Los Miembros de las BCR reconocen que dicho reclamo podrá interponerse ante el Estado miembro en el que esté establecido el Miembro de las BCR responsable del incumplimiento o ante el tribunal en el que el Titular de los Datos tenga su residencia habitual.

Concentrix será responsable de demostrar que dicho miembro de las BCR fuera del EEE no es responsable de ninguna violación de las reglas especificadas en estas BCR-P y que hayan resultado en reclamo de daños por parte del Titular de los Datos. En caso de que Concentrix pueda demostrar que el otro miembro de las BCR ubicado fuera del EEE no fue responsable del acto, entonces podrá eximirse de cualquier responsabilidad.

Cuando el Responsable pueda demostrar que ha sufrido daños y pruebas de que los daños se han producido probablemente debido a una infracción de estas BCR-P por parte de un Miembro de las BCR fuera del EEE, Concentrix será responsable de demostrar que el Miembro de las BCR fuera del EEE o el Subencargado externo fuera del EEE no fue responsable de la infracción de las BCR-P que dio lugar a los daños en cuestión o que no se produjo tal infracción.

7.4 Derechos de los Titulares de los Datos

Los Titulares de los Datos tienen derecho a beneficiarse de los siguientes derechos:

- Tener acceso a los Datos Personales que le conciernen y que son tratados por un miembro de las BCR.

- Solicitar la rectificación o supresión de cualquier Dato Personal inexacto o incompleto que le concierna, así como de cualquier Dato Personal respecto del cual la finalidad del Tratamiento ya no sea lícita o adecuada; es:
- Solicitar que el Tratamiento de sus Datos Personales sea limitado.
- Oponerse al Tratamiento de los Datos de los Titulares por parte de un miembro de las BCR cuando dicho Tratamiento sea necesario para los fines de los intereses legítimos perseguidos por el Responsable de los Datos, para fines de intereses legítimos, incluyendo la elaboración de perfiles en cualquier momento, por motivos relacionados con su situación personal, a menos que los intereses perseguidos por el Cliente, actuando como Responsable de los Datos, prevalezcan sobre los intereses, derechos y libertades de los Titulares de los Datos.
- Oponerse al Tratamiento de los Datos de los Titulares por parte de un miembro de las BCR cuando dicho Tratamiento sea necesario para los fines de los intereses legítimos perseguidos por el Responsable de los Datos o por un tercero, para fines de marketing, incluida la elaboración de perfiles; y
- Recibir sus Datos Titulares en un formato estructurado, de uso común, legible por máquina e interoperable cuando el Tratamiento se realice por medios automatizados.

Cuando un miembro de las BCR actúe como Encargado de los Datos y reciba una solicitud de los Titulares de los Datos para ejercer sus derechos, el miembro de las BCR deberá informar a su Cliente, y este último deberá responder a la solicitud. Un miembro de las BCR solo será responsable de seguir las instrucciones adicionales de su Cliente sobre cómo manejar dicha solicitud. Los miembros de las BCR ejecutarán cualquier medida necesaria solicitada por el Cliente para que los Datos Personales sean actualizados, corregidos, eliminados o anonimizados desde el momento en que el formulario de identificación ya no sea necesario. Los miembros de las BCR deberán comunicar estas instrucciones a cualquier miembro relevante de las BCR a quien se hayan divulgado los Datos Personales. Los miembros de las BCR también ejecutarán las medidas técnicas y organizativas apropiadas, en la medida en que esto sea posible, siguiendo las instrucciones del Cliente, para cumplir con su obligación de responder a las solicitudes, incluso comunicando cualquier información útil. Cuando el Cliente haya desaparecido, dejado de existir o se haya vuelto insolvente, el miembro relevante de las BCR deberá manejar directamente dicha solicitud en la medida de lo posible y según el procedimiento que haya adoptado.

7.5 Ejercicio de los Derechos de los Titulares de Datos

Los Titulares de los Datos tienen derecho a hacer cumplir estas BCR-P como beneficiarios de terceros y a ejercer sus derechos con respecto al Tratamiento de los Datos los Titulares por cualquier miembro de las BCR que actúe como Encargado de los Datos. El miembro de las BCR deberá asegurarse de que cualquier solicitud o queja de los Titulares de los Datos relacionada con el ejercer de sus derechos (**“Solicitudes”**) se aborde de manera oportuna.

Los Titulares de los Datos pueden hacer una solicitud verbalmente o por escrito. Los miembros de las BCR proporcionarán a los Titulares de los Datos medios accesibles para ejercer sus derechos y, en particular:

1 - Un correo electrónico de contacto único que se utilizará independientemente del país en el que se encuentre el Titular de los Datos:

Proteccion.dedatos@concentrix.com y dpo@concentrix.com

Se pueden utilizar correos electrónicos locales para tener en cuenta especificidades locales, como el idioma.

Para ponerse en contacto con su contacto local de privacidad, consulte el Apéndice 01 - Lista de entidades de Concentrix obligadas por el BCR-P y contactos locales de privacidad por correo electrónico.

2 - Portal único con la dirección de correo electrónico del RPD de Concentrix accesible a través de un enlace en www.concentrix.com

3 - Dirección postal única que se utilizará independientemente del país en el que se encuentre el Titular de los Datos:

Group Data Privacy Officer

Legal and Compliance Department

3 rue d'Heliopolis

75017 – PARIS

FRANCIA

El DPO, o cualquier otra persona o entidad, interna o externa, designada por el DPO para gestionar las Solicitudes, deberá (i) asegurarse de que haya obtenido la información mínima requerida del Titular de los Datos para abordar su Solicitud y (ii), si se considera necesario, obtener la mayor cantidad de información posible para que la Solicitud sea gestionada adecuadamente.

Si existe alguna duda sobre la identidad de la persona que hace la solicitud, principalmente cuando se utilizan medios de comunicación a distancia, un miembro de las BCR puede solicitar más información sobre el Titular de los Datos. La información recopilada deberá (i) limitarse a la información necesaria para confirmar quién es la persona que realiza la solicitud y (ii) no se deberá recopilar cuando los productos o servicios proporcionados por un miembro de las BCR o sus Clientes no se entreguen bajo la identidad real del usuario. La proporcionalidad siempre será evaluada por el Responsable de los Datos.

En cualquier caso, la respuesta a un Titular de los Datos debe ocurrir dentro de un plazo máximo de 1 mes después de recibir la Solicitud. Teniendo en cuenta la complejidad y el número de solicitudes, ese mes puede extenderse como máximo dos meses adicionales, en cuyo caso se debe informar al reclamante en consecuencia (como se detalla en el Apéndice 6).

Cuando el Titular de los Datos no esté satisfecho con la respuesta inicial proporcionada por el miembro de las BCR, el Titular de los Datos tendrá derecho a solicitar de inmediato que se reconsidere su Solicitud. El Titular de los Datos deberá proporcionar al miembro de las BCR una explicación detallada de las disposiciones insatisfactorias de la solución previamente proporcionada. El miembro de las BCR no deberá tardar más de 2 meses desde la recepción de la Solicitud de

reconsideración en determinar cómo se manejará y deberá informar al Titular de los Datos por escrito en consecuencia.

Si una Solicitud o queja del Titular de los Datos es rechazada por el miembro de las BCR o si la respuesta no satisface al Titular de los Datos, el Titular de los Datos podrá contactar al DPO y/o presentar una queja directamente ante un Órgano de Vigilancia competente del EEE y/o buscar un remedio judicial.

Detalles adicionales sobre este Artículo están disponibles en el siguiente apéndice:

- **Apéndice 6 - Procedimiento para las solicitudes de los Titulares de los Datos cuando Concentrix actúa como Encargado de los Datos.**

8. Proceso para el manejo de denuncias de los Titulares de los Datos

Cuando el Titular de la Información comunique una queja directamente a un Miembro de las BCR, pero el cliente no ha dejado de existir, no ha desaparecido u no se ha vuelto insolvente al momento en que dicha solicitud fue recibida por el Miembro de las BCR, entonces el Miembro de las BCR se compromete a informar al cliente sobre dicha solicitud sin demora y de acuerdo con el procedimiento definido en el **Apéndice 6 – Procedimiento para las solicitudes de los Titulares de la Información donde Concentrix actúa como el Encargado de los Datos**

En tal caso, el Miembro de las BCR se compromete a comunicar cualquier información relevante que reciba del Titular de la Información para el Cliente, y está de acuerdo en indicar expresamente al Cliente que es la responsabilidad del Cliente manejar dicha queja.

Concentrix no es responsable del manejo de quejas hechas por los Titulares de la Información cuando actúe como Encargado de los Datos. Sin embargo, en caso de que el cliente haya desaparecido de hecho, haya dejado de existir bajo la ley o se haya declarado insolvente, los Miembros de las BCR se comprometen a manejar las quejas de los Titulares de la Información de acuerdo con el mismo procedimiento que se especifica en el Artículo 8 de las BCR-P. En este caso, Los miembros de las BCR reconocen que los Titulares de la Información siguen teniendo derecho a presentar una reclamación ante a un Órgano de Vigilancia del EEE y/o a buscar recursos judiciales. Los Miembros de las BCR también reconocen que dichos derechos no dependen de que los Titulares de la Información hayan usado con antelación el proceso para el manejo de denuncias, sin embargo, se incentiva a los Titulares de la Información a hacerlo.

9. Quejas de Clientes Externos

Cuando un miembro de las BCR que actúe como Encargado de los Datos no cumpla con estas BCR-P, Concentrix reconoce que el Cliente tiene el derecho a hacer cumplir estas BCR-P en contra de un Miembro de las BCR que no las cumpla.

El Cliente tendrá derecho a recursos judiciales y tiene el derecho a recibir compensación del Miembro de las BCR que haya originado la violación, conforme a lo dispuesto en el Acuerdo de Servicio y/o en el Acuerdo de Procesamiento de los Datos.

10. Gobernanza de protección de datos

Concentrix ha definido una organización y gobernanza de la protección de Datos, la cual se define más a fondo en el Apéndice 3.

Los miembros de las BCR se comprometen a designar un Oficial de Privacidad de Datos, donde se requiera y, en línea con el Artículo 37 RGPD, o cualquier otra persona o entidad (como el oficial encargado de la privacidad) con la responsabilidad de monitorear el complimiento de las BCR-P y goza del más alto apoyo administrativo para el cumplimiento de esta tarea. Esta organización es dirigida por el Oficial de Privacidad del Grupo, quien depende de una red de puntos de contacto de privacidad (específicamente los Líderes Regionales de Privacidad, Líderes Locales de Privacidad, además de los Referentes de Privacidad del Negocio) y quienes pueden ser designados como DPO por el miembro competente de las BCR.

El DPO nombrado formalmente con un Órgano de Vigilancia debe reportarse directamente con el nivel más alto de dirección. Adicionalmente, el DPO puede informar al nivel más alto de dirección si surge cualquier pregunta o problema durante el ejercicio de sus funciones.

El DPO no debe tener tareas que puedan dar lugar a conflictos de intereses. El DPO no debe encargarse de realizar evaluaciones del impacto de la protección de datos, y tampoco debe encargarse de realizar auditorías de las BCR si dicha situación resulta en un conflicto de intereses. Sin embargo, El DPO puede desempeñar un papel muy útil e importante al asistir a los miembros de las BCR, y se deben pedir sugerencias del DPO.

Los roles y responsabilidades de la red, así como su gobernanza de trabajo son definidos en detalle en el **Apéndice 3 – Organización y gobernanza de la protección de datos**.

Adicionalmente, el DPO puede informar al nivel más alto de dirección si surgen preguntas o problemas durante el ejercicio de sus funciones.

El DPO y los Líderes Locales y Regionales de Privacidad pueden ser contactados a través de la información de contacto descrita en el Artículo 7.5 de las BCR-C y en los contactos de privacidad local suministrados en el Apéndice 01 de las BCR.

11. Entrenamiento y sensibilización

Proteger los Datos Personales no es sólo cuestión de cumplir con las leyes de privacidad, sino que hace parte de la materialización de los valores fundamentales de Concentrix. En este contexto, promover una cultura de la privacidad dentro del grupo es esencial para hacer que todos los empleados, aprendices, y otras personas cuyas conductas en el ejercicio de sus funciones estén bajo el control directo de los

Miembros de las BCR, sean responsables de la protección de Datos Personales procesados como parte de sus operaciones.

Por lo tanto, estas BCR-P deben ser implementadas apropiadamente al interior de toda la organización. Para tal fin, los Miembros de las BCR han adoptado un programa de entrenamiento en privacidad, con el objetivo de asegurar que los empleados de Concentrix, aprendices, y otras personas cuya conducta, en el ejercicio de sus funciones estén bajo el control directo de los Miembros de las BCR, realmente están al tanto de las obligaciones, principios y procedimientos especificados en estas BCR-P. Además de los principios y obligaciones claves de la RGPD, el programa de entrenamiento y sensibilización debe cubrir, entre otros, los procedimientos para manejar solicitudes de acceso a la información personal por parte de las autoridades públicas.

Dicho entrenamiento está dirigido a: (i) personas que tengan acceso permanente o regular a los Datos Personales; (ii) personas involucradas en la recolección de Datos Personales; y/o (iii) personas involucradas en el desarrollo de herramientas utilizadas para procesar Datos Personales.

El material de capacitación deberá estar actualizado y revisarse periódicamente, al menos una vez al año o cuando se produzcan cambios significativos en la legislación de protección de datos aplicable, a fin de garantizar que refleje la última versión del BCR-P.

El programa de entrenamiento apuntará a proporcionar:

- Un nivel básico de conocimiento fundamental de los principios que aplican al momento de Procesar los Datos Personales y un buen conocimiento de los procesos existentes y su implementación, y
- Entrenamiento específico adaptado a las diferentes funciones dentro de la organización.

En este sentido, se recuerda que los Miembros de las BCR reconocen que no se puede hacer ninguna transferencia bajo las BCR-P a otro Miembro de las BCR, a menos que este último sea vinculado efectivamente por las BCR-P y se pueda proporcionar un entrenamiento efectivo sobre las BCR-P a los empleados del respectivo Miembro de las BCR.

Los Miembros de las BCR se comprometen a asegurar que todos los empleados de Concentrix, sus aprendices y otras personas cuyas conductas, que en el ejercicio de su trabajo estén bajo control directo de los Miembros de las BCR, tomen el entrenamiento una vez esté disponible y, posteriormente, completen el curso de actualización anual.

En el siguiente apéndice se encuentran más detalles con respecto a este artículo:

- **Apéndice 04 – Programa de entrenamiento y sensibilización.**
-

12. Privacidad por diseño / privacidad por defecto

Cuando actúen como Encargados de los Datos, los Miembros de las BCR deben seguir cualquier instrucción razonable del Cliente para permitir que este último cumpla con sus obligaciones adjuntas a la Privacidad por diseño y a la Privacidad por defecto.

13. Transparencia y Cooperación

13.1 Comunicación de las BCR-P

Los Miembros de las BCR se compromete a asegurar que a todos los Titulares de los Datos se les proporcione información sobre sus derechos de beneficiarios terciarios, con respecto al procesamiento de sus Datos Personales, y sobre los medios para ejercer esos derechos. Dicha información se describe en el Artículo 7 de las BCR-P.

Concentrix comunicará abiertamente estas BCR-P a los Titulares de los Datos y las hará fácilmente accesible para cualquier persona. Dicha comunicación debe permitirle a cualquier Titular de los Datos obtener una copia de estas BCR-P sin demoras injustificadas y en un formato abierto.

Adicionalmente, una versión pública de la última versión de las BCR-P actuales debe estar disponible en cualquier momento para los Titulares de los Datos en el sitio web de Concentrix www.concentrix.com. Los Titulares de los Datos también puede solicitar una copia de las BCR-P contactando al DPO en dpo@concentrix.com.

La versión pública de las BCRs-P debe contener, al menos, la siguiente información:

- Una descripción del alcance de las BCR-P (Artículo 2 de las BCR-P),
- La cláusula relacionada con las responsabilidades del Grupo (Artículo 7 de las BCR-P),
- Las cláusulas relacionadas con los principios de protección de datos (Artículo 4, y 5 de las BCR-P),
- Notificaciones de seguridad y de violaciones a la información personal (Artículo 4.5 de las BCR-P)
- Sub encargado y las restricciones en transferencias ulteriores (Artículo 4.7 y Artículo 6 de las BCR-P), y
- Las cláusulas relacionadas con los derechos de los Titulares de los Datos (Artículo 7, 8 y 13 de las BCR-P).

Esta información debe ser actualizada y presentada a los Titulares de los Datos de una manera clara, inteligible y transparente. Esta información debe ser proporcionada de manera completa, por consiguiente, un resumen de este documento no será suficiente.

La versión pública también debe incluir todas las políticas y procedimientos requeridos adjuntos a las BCR-P como Apéndice, especialmente para las BCR-P:

- Apéndice 01-A Lista de Miembros de las BCR vinculados por las BCR-P y los correos electrónicos de contacto de privacidad local
- Apéndice 02 Definiciones para las BCR y procedimientos
- Apéndice 06 Procedimiento para las solicitudes de los Titulares de los Datos donde Concentrix actúa como Encargado de los Datos.
- Apéndice 11-B Alcance material de las BCR-P: Lista de propósitos del procesamiento y las categorías relacionadas con los Datos Personales y los Titulares de los Datos.
- Apéndice 12 Contrato Marco de Procesamiento de Datos Personales

Los otros Apéndices, o bien no son aplicables a las BCR-C, o bien son procesos internos irrelevantes para que los Titulares de los Datos entiendan o ejerzan sus derechos.

Estos requerimientos anteriores serán cumplidos al asegurar que la versión pública simplificada de las BCR-P, que contiene toda la información listada anteriormente, esté disponible en el sitio web de Concentrix (www.concentrix.com).

Cuando actúen como Encargados de los Datos, los miembros de las BCR se comprometen a compartir estas BCR-P con sus clientes y deben incluir estas BCR-P en el Acuerdo de Servicio para divulgar y hacer cumplir las BCR-P. En cualquier caso, cuando actúen como Encargados de los Datos, como se menciona en el artículo 3 y 4 de esta BCR-P, los miembros de las BCR se comprometen a cumplir con las BCR-P con relación al Procesamiento de los Datos Personales de su Cliente.

13.2 Información a los titulares de los datos

Cuando actúen como Encargados de los Datos, los Miembros de las BCR son responsables de proporcionar a sus Clientes la información pertinente que les permita facilitar a los Titulares de los Datos la información relevante exigida por la Legislación Aplicable sobre Protección de Datos.

Sin embargo, los Miembros de las BCR no serán responsables de proporcionar la información obligatoria a los Titulares de los Datos según lo requerido por la Legislación Aplicable sobre Protección de Datos, ya que los Clientes de los Miembros de las BCR son los únicos responsables a este respecto.

13.3 Inconsistencias con la legislación y las prácticas locales que afectan al cumplimiento de las BCR-P

Los miembros de las BCR se comprometen a utilizar las BCR-P como herramienta para las transferencias únicamente cuando hayan evaluado que la legislación y las prácticas de un País Tercero No Adecuado aplicables al tratamiento de los datos personales por parte del miembro de las BCR que actúa como Importador de los Datos, incluido cualquier requisito de revelación de datos personales o medidas que autoricen el acceso de las autoridades públicas, no le impiden cumplir sus obligaciones en virtud de estas BCR-P.

Dicho compromiso se basa en el entendimiento de que las leyes y prácticas – que respetan la esencia de los derechos y libertades fundamentales, y no exceden lo que es necesario y proporcionado en una sociedad democrática para salvaguardar uno de los fines enumerados a continuación – no están en contradicción con el BCR-P:

(k) seguridad nacional, y/o,
(l) la defensa, y/o
(m) la seguridad pública, y/o

(n) la prevención, investigación, detección o enjuiciamiento de delitos o la ejecución de sanciones penales, incluida la protección y prevención de amenazas a la seguridad pública; y/o
(o) otros objetivos importantes de interés público general de la Unión o de un Estado Miembro, en particular un interés económico o financiero importante de la Unión o de un Estado Miembro, incluidos los asuntos monetarios, presupuestales y fiscales, la salud pública y la seguridad social; y/o
(p) la protección de la independencia judicial y de los procedimientos judiciales; y/o
(q) la prevención, investigación, detección y procesamiento judicial de las violaciones a la ética de las profesiones reguladas; ad/o
(r) una función de control, inspección o reglamentación vinculada, incluso ocasionalmente, al ejercicio del poder público en los casos contemplados en las letras a) a e) y g); y/o
(s) la protección del Titular de los datos o de los derechos y libertades de terceros; y/o
(t) la ejecución de reclamaciones de derecho civil.

Al evaluar las leyes y prácticas del País Tercero No Adecuado que puedan afectar al respeto de los compromisos contenidos en las BCR-P, los Miembros de las BCR tendrán debidamente en cuenta, en particular, los siguientes elementos:

- **Las circunstancias específicas de las Transferencias** o conjunto de transferencias, y de cualquier transferencia posterior prevista dentro del mismo tercer país o a otro País Tercero No Adecuado, incluyendo:

  - fines para los cuales se transfieren y tratan los Datos Personales (por ejemplo, almacenamiento, soporte TI, servicios de externalización de procesos empresariales como la atención al cliente en nombre del Cliente);
  - tipos de entidades implicadas en el Tratamiento (el Importador de los Datos y cualquier otro destinatario de cualquier Transferencia ulterior)
  - sector económico en el que se produce la Transferencia o conjunto de Transferencias;
  - las categorías y formato de los Datos Personales Transferidos
  - lugar del tratamiento, incluido el almacenamiento; y
  - canales de transmisión utilizados.

- **Las leyes y prácticas del País Tercero de destino** pertinentes a la luz de las circunstancias de la Transferencia, incluidas las que exigen revelar datos a las autoridades o autorizan el acceso de dichas autoridades y las que proveen el acceso a estos Datos Personales durante el tránsito entre el país del Exportador de los Datos y el país del Importador de los Datos, así como las limitaciones y salvaguardias aplicables.
- **Todas las salvaguardas contractuales, técnicas u organizativas pertinentes** establecidas para complementar las salvaguardias en virtud de las BCR-P, incluidas las medidas aplicadas durante la transmisión y el Tratamiento de los Datos Personales en el país de destino.

Teniendo en cuenta lo anterior, cuando un miembro de las BCR tenga motivos para creer que su legislación local le impide cumplir con sus obligaciones en virtud de estas BCR-P, incluido cualquiera de los principios de tratamiento. anterior y tenga un efecto sustancial sobre las garantías aquí suministradas, dicho miembro de las BCR deberá informar sin demora (i) a su(s) cliente(s), (ii) a Concentrix, (iii) al miembro de las BCR de la UE con responsabilidades delegadas en materia de protección de datos y (iv) al DPO o al correspondiente Líder Local de Privacidad/otra función de privacidad.

Cuando un miembro de las BCR actúe como Encargado de los Datos, también se compromete a notificarlo sin demora a la autoridad de protección de datos competente para su cliente en tal caso.

En caso de que se haya informado a los puntos de contacto pertinentes de los miembros de las BCR de acuerdo con el mecanismo de notificación mencionado anteriormente, Concentrix lo notificará al Órgano de Vigilancia competente del EEE. En tal caso, Concentrix se compromete a notificar este requisito legal al Órgano de Vigilancia competente del EEE sin demoras indebidas y, en caso de que dicho requisito legal exija la divulgación de Datos Personales por parte del Miembro de las BCR en cuestión, a divulgar únicamente los Datos Personales necesarios de conformidad con la legislación local pertinente. Los miembros de las BCR especificarán a qué Titular de los Datos puede afectar este requisito legal o revelación, qué autoridad solicita esta revelación y sobre qué base legal se fundamenta. En cualquier caso, los miembros las BCR se comprometen a no transferir datos personales a las autoridades públicas de forma masiva, indiscriminada y desproporcionada.

Si un Miembro de las BCR tiene legalmente prohibido llevar a cabo dicha notificación, deberá hacer todo lo posible por eludir dicha prohibición de conformidad con la legislación local aplicable. Concentrix y este Miembro de las BCR harán todo lo posible por eludir dicha prohibición para notificar al Cliente y a las Autoridades de Supervisión del EEE pertinentes. Para demostrar su mejor esfuerzo para eludir la prohibición, los Miembros de las BCR documentarán las medidas adoptadas para tal fin y las pondrán a disposición del Órgano de Vigilancia del EEE pertinente. Cuando no sea posible eludir dicha prohibición, Concentrix deberá proporcionar anualmente información general sobre las cifras de divulgación de Datos Personales a las autoridades pertinentes (por ejemplo, número de solicitudes de divulgación, tipo de datos solicitados, el solicitante si es posible, etc.).

Además, cuando un Miembro de las BCR esté sujeto a la legislación nacional de los Estados miembros de la UE que añada algunos requisitos o modalidades que puedan tener un impacto en el Tratamiento llevado a cabo por un Miembro de las BCR en virtud de estas BCR-P, este Miembro de las BCR informará sin demora a Concentrix y documentará los requisitos complementarios aplicables en virtud de esta legislación nacional. Cuando esta legislación nacional imponga un mayor nivel de protección a los Datos Personales, esta legislación nacional prevalecerá sobre las BCR-P.

Cuando un miembro de las BCR ubicado fuera del EEE tenga motivos para creer que está o ha estado sujeto a leyes o prácticas que no se ajustan a la evaluación antes mencionada, deberá notificarlo sin demora al cliente o al miembro de las BCR

de la UE que actúe como Encargado de los Datos en nombre de dicho Cliente, que remitirá la notificación al Cliente. Tras la notificación, el Cliente y/o el Miembro de las BCR de la UE que actúe como Encargado de los Datos deberán identificar sin demora las medidas apropiadas (por ejemplo, medidas técnicas u organizativas para garantizar la seguridad y la confidencialidad) que deberán adoptarse para hacer frente a la situación. Si no pueden garantizarse las salvaguardias adecuadas para dicha Transferencia, ésta deberá suspenderse. En ese caso, el Cliente y/o Miembro de las BCR de la UE tendrán derecho a rescindir el contrato, si afecta al tratamiento de datos personales según BCR-P. Si el contrato implica a más de dos partes, el Cliente y/o el Miembro de las BCR de la UE podrán ejercer este derecho de rescisión solo con respecto al Miembro de las BCR pertinente que no pueda garantizar un nivel adecuado de protección de datos personales, salvo que las partes hayan acordado otra cosa.

13.4 Deber de cooperar

En cualquier caso, los miembros de las BCR se comprometen a cooperar con las Autoridades de Supervisión del EEE, incluso aceptando ser auditados o inspeccionados (en las instalaciones o a distancia) por dichas Autoridades de Supervisión, a tener en cuenta el asesoramiento y a acatar la decisión del Órgano de Vigilancia del EEE competente que pueda ser proporcionada en relación con estas BCR-P. Los miembros de las BCR reconocen y aceptan que los poderes y derechos de auditoría del Órgano de Vigilancia competente no pueden ser limitados, en particular en relación con la auditoría práctica llevada a cabo por dicho Órgano de Vigilancia.

Cuando actúen como Encargados de los Datos, los miembros de las BCR se comprometen a cooperar en un plazo razonable y en la medida de lo razonablemente posible con sus Clientes y a ayudarles a cumplir la Legislación Aplicable sobre Protección de Datos. Los miembros de las BCR también se asegurarán de que cualquier sub procesador que utilicen para procesar datos personales esté obligado a cumplir con el mismo deber de cooperar y ayudar a los miembros de las BCR y, según sea necesario, al Responsable de los Datos.

Los miembros de las BCR y, cuando corresponda, sus respectivos representantes pondrán a disposición del Órgano de Vigilancia del EEE, previa solicitud, cualquier información sobre las operaciones de tratamiento cubiertas por las BCR-P, como los registros de las actividades de tratamiento.

Cualquier disputa relacionada con el ejercicio de supervisión del cumplimiento de las BCR-P por parte de la Órgano de Vigilancia competente será resuelta por los tribunales del Estado Miembro de dicho Órgano de Vigilancia, de conformidad con la legislación procesal de dicho Estado Miembro. Los miembros de las BCR aceptan someterse a la jurisdicción de estos tribunales.

14. Programa de auditoría que abarca las BCR

Cada miembro de las BCR que actúe como Encargado será responsable del cumplimiento de las BCR-P y estará en condiciones de demostrarlo. A tal fin, y además de los requisitos establecidos en el artículo 4.4 (Registro de actividades de tratamiento) y en el artículo 4.5 (Seguridad), los miembros de las BCR deberán cumplir el siguiente requisito relativo al programa de auditoría de protección de datos.

El miembro de las BCR se compromete a desarrollar e integrar en su programa de auditoría la revisión de su cumplimiento con estas BCR-P. El programa de auditoría permitirá definir:

- una frecuencia razonable con la que se llevarán a cabo las auditorías
- el alcance previsto de la auditoría; y
- el equipo encargado de la auditoría.

El procedimiento de auditoría se detalla en el **Apéndice 7 - Procedimientos para las Auditorias de Privacidad de los Datos**. La auditoría abarca todos los aspectos de estas BCR-P (por ejemplo, aplicaciones, sistemas TI, bases de datos que procesan datos personales, o transferencias ulteriores, decisiones tomadas con respecto a los requisitos obligatorios en virtud de leyes nacionales que entran en conflicto con las BCR-P, la revisión de las condiciones contractuales utilizadas para las transferencias fuera del Grupo a los Encargados de los Datos, las medidas correctivas, etc.), incluyendo los métodos y planes de acción que garanticen que se llevarán a cabo las medidas correctivas. Sin embargo, no es necesario que dicho programa de auditoría, necesariamente, monitoree todos los aspectos de las BCR-P cada vez que se audita a un miembro de las BCR, siempre y cuando todos los aspectos de las BCR-P se supervisen a intervalos regulares adecuados para dicho Miembro de las BCR.

Los miembros de las BCR se comprometen a realizar auditorías de forma periódica (al menos una vez al año y/o si existen indicios de incumplimiento) para garantizar la verificación del cumplimiento de las BCR-P o considerando el nivel de riesgo de una actividad de Tratamiento cubierta por las presentes BCR-P para los derechos y libertades de los Titulares de los Datos.

Además de las auditorías periódicas, el DPO y/o el miembro pertinente de la red de privacidad (por ejemplo, el Líder Local de Privacidad), o cualquier otra función competente del grupo Concentrix, como el departamento de auditoría interna, podrán solicitar auditorías específicas (auditorías ad hoc). Dichas auditorías podrán ser realizadas por auditores acreditados internos y/o externos asesorados por el DPO y/o el miembro de la red de privacidad pertinente. La hoja de ruta la iniciará y determinará el DPO y/o el miembro pertinente de la red de privacidad, tal como se especifica en el apéndice 7. En cualquier caso, los auditores externos serán independientes y estarán sujetos a una obligación de confidencialidad y/o a una obligación legal de confidencialidad adecuada.

El DPO es responsable de determinar el alcance de las auditorías que deben realizarse. Para ello, puede consultar al Comité de Privacidad y/o encargar al equipo de auditoría interna de Concentrix que determine el alcance de dicha auditoría. La auditoría podrá ser realizada por el DPO del grupo y/o los miembros pertinentes de la red de privacidad (por ejemplo, el Líder Local de Privacidad) y/o por el equipo de

auditoría interna del grupo Concentrix o cualquier otra función pertinente dentro de Concentrix siempre que:

- Se garantice la independencia de los responsables en el ejercicio de sus funciones para estas auditorías; y
- Las personas encargadas de auditar el cumplimiento de las BCR-P, si tal situación da lugar a un conflicto de intereses.

Los resultados de cada auditoría se presentarán al DPO del Grupo y/o a los miembros pertinentes de la red de privacidad (por ejemplo, los Líderes Locales de Privacidad) y/o al Comité de Privacidad y/o a los miembros de la junta directiva de Concentrix para su información. El informe final, la identificación de defectos y las medidas correctivas serán compartidas y aplicadas por el Líder Local de Privacidad. Basándose en la evaluación del Líder Local de Privacidad, el informe también podrá compartirse, cuando sea apropiado, con cualquier Referente de Privacidad del Negocio, con el gerente de seguridad local, con los propietarios del proceso/sistema, la junta directiva matriz del grupo Concenrix o la junta directiva del miembro de las BCR pertinente sujeto a la auditoría o cualquier otro empleado interno necesario. Se definirán medidas correctoras con un orden de prioridades para determinar un calendario para la implementación de dichas medidas.

Concentrix reconoce que los Órganos de Vigilancia competentes del EEE, así como los Clientes de los Miembros de las BCR, si se ven directamente afectados por la auditoría, pueden solicitar la comunicación de los resultados de la auditoría y, por lo tanto, se compromete a concederles acceso a los mismos si así lo solicitan. Los resultados de los informes de auditoría y los informes de auditoría interna relevantes se mantendrán de forma que los Órganos de Vigilancia situados en el EEE puedan acceder a ellos si utilizan su derecho de auditoría establecido más adelante. Además, los miembros de las BCR que actúen como Encargados o Sub encargados de los Datos se comprometen a presentar, a petición del Responsable de los Datos, sus instalaciones de tratamiento de datos para la auditoría de las actividades de tratamiento relativas al Responsable de los Datos.

Los miembros de las BCR se comprometen a garantizar que los Órganos de Vigilancia Competentes puedan tener acceso a los resultados de la auditoría, previa solicitud y no limitarán tales derechos, especialmente por motivos de confidencialidad, por ejemplo, en relación con la protección de secretos del negocio.

Se recuerda que el Miembro de las BCR autorizará a cualquier Órgano de Vigilancia competente del EEE a llevar a cabo por sí misma auditorías de protección de datos sobre cualquier cuestión relacionada con las BCR-P. A este respecto, cada miembro de las BCR permitirá al Órgano de Vigilancia del EEE auditar al miembro de las BCR pertinente con el fin de que el Órgano de Vigilancia del EEE pueda obtener la información necesaria para demostrar el cumplimiento de estas BCR-P por parte del miembro o miembros de las BCR (véase también el artículo 13.4 anterior).

Además, cuando un Miembro de las BCR actúe como Encargado de los Datos, sus Clientes podrán solicitar, previo aviso con una periodicidad razonable y en cualquier caso no más de una vez al año, y a su propio coste, que Concentrix lleve a cabo auditorías para evaluar su cumplimiento o el cumplimiento de sus sub encargados con el Contrato de Servicios y/o del Contrato de Tratamiento de los Datos, así como del presente BCR-P.

En este caso, el Miembro de las BCR deberá poner a disposición del Cliente toda la información necesaria para demostrar el cumplimiento de la Legislación Aplicable sobre Protección de Datos, estas BCR-P y el Acuerdo de Tratamiento de Datos aplicable y permitir y contribuir a las auditorías, incluidas las inspecciones, realizadas por el Cliente u otro auditor encargado por el Cliente de conformidad con el Acuerdo de Servicio.

Dicha Auditoría cumplirá con el procedimiento establecido en el Apéndice 07.

15. Cambios a las BCR-P

El DPO de Concentrix, con el apoyo de los Líderes Locales de Privacidad, se asegurarán de que las presentes BCR-P se mantengan actualizadas (por ejemplo, teniendo en cuenta las modificaciones del entorno regulatorio, las recomendaciones de las autoridades de protección de datos de la UE, o los cambios en el alcance de las BCR-P).

Particularmente, el DPO mantendrá actualizada una lista de entidades vinculadas por las BCR-P. Cuando una nueva entidad de Concentrix quede efectivamente vinculada por las BCR-P (como se especifica en el artículo 3.2), el DPO actualizará la lista e informará sin demora indebida a todos los miembros de las BCR y a los Órganos de Vigilancia pertinentes del EEE a través del Órgano de Vigilancia competente del EEE. Dicha información actualizada se pondrá a disposición de los Titulares de los Datos junto con el BCR-P y por los mismos medios.

Al menos una vez al año, o cuando el DPO lo considere necesario, Concentrix notificará dichos cambios a los Órganos de Vigilancia competentes del EEE. La notificación de dichos cambios a los Órganos de Vigilancia del EEE se realizará al menos una vez al año a través del Órgano de Vigilancia del EEE competente con una breve explicación de los motivos que justifican la actualización. Los Órganos de Vigilancia también deberán ser notificados una vez al año, siguiendo el mismo proceso, en casos de que no se hayan hecho cambios.

La actualización o notificación anual también deben incluir la renovación de la confirmación relativa al hecho de que Concentrix, como Miembro Responsable de las BCR, ha tomado las medidas apropiadas para permitirse el pago de una indemnización por cualquier daño resultante de una violación a las BCR-P por parte de los Miembros de las BCR fuera del EEE.

En la misma medida, cuando una enmienda tenga un impacto sustancial en las BCR-P o en el nivel de protección de los derechos otorgados por estas BCR-P, Concentrix, con la asistencia del DPO, se compromete a informar sin demora a los Miembros de las BCR y a los Órganos de Vigilancia del EEE.

16. Incumplimiento con las BCR-P

Al convertirse en miembro de las BCR, el Exportador y el Importador de los Datos deberán cumplir con los siguientes requisitos:

- No se realizará ninguna transferencia a un miembro de las BCR a menos que el miembro de las BCR esté efectivamente vinculado por las BCR-P y pueda cumplirlas.

- El Importador de los Datos deberá informar sin demora al Exportador de los Datos si no puede cumplir las BCR-P, por el motivo que sea, incluidas las situaciones descritas con mayor detalle en el artículo 13.3 de las BCR-P.
- Si el Importador de los Datos incumple las BCR-P o no puede cumplirlas, el Exportador de los Datos o el Cliente deberán suspender la Transferencia.

El Importador de los Datos deberá, a elección del Exportador de los Datos, devolver o borrar inmediatamente los Datos Personales que hayan sido Transferidos en virtud de las BCR-P en su totalidad, cuando:

- El Exportador de los Datos haya suspendido la transferencia y no se restablece el cumplimiento de estas BCR-P en un plazo razonable y, en cualquier caso, en el plazo de un mes desde la suspensión; o bien

- El Importador de los Datos incumpla de forma sustancial o persistente las BCR-P; o
- El Importador de los Datos incumpla una decisión vinculante de un tribunal competente o de un Órgano de Vigilancia competente con respecto a sus obligaciones en virtud de las BCR-P.

Los mismos compromisos deberán aplicarse a cualquier copia de los datos. El Importador de los Datos deberá certificar la eliminación de los datos al Exportador de los Datos.

Hasta que los datos sean eliminados o devueltos, el Importador de los Datos deberá seguir garantizando el cumplimiento de las BCR-P.

En caso de que la legislación local aplicable al Importador de los Datos prohíba la devolución o eliminación de los datos personales transferidos, el Importador de los Datos deberá garantizar que seguirá velando por el cumplimiento de las BCR-P, y que sólo tratará los datos en la medida y durante el tiempo que exija dicha legislación local.

Para los casos en que las leyes y/o prácticas locales aplicables afecten al cumplimiento de las BCR-P, véase el artículo 13.3 de las BCR-P mencionado anteriormente.

17. Terminación

Un miembro de las BCR que actúe como Importador de los Datos y que deje de estar vinculado por las BCR-P podrá conservar, devolver o eliminar los datos personales recibidos en virtud de las BCR-P.

Si el Exportador de los Datos y el Importador de los Datos acuerdan que los datos pueden ser conservados por el Importador de los Datos, la protección debe mantenerse en línea con el Capítulo V GDPR y como se refleja en el Artículo 6 de las BCR-P.

CONTROL DE DOCUMENTO

Versión	Actualización	Resumen de modificaciones
0.1	27/02/2022	Aprobación final
0.2	01/01/2023	Actualización de la lista de Miembros de las BCR
0.3	24/02/2023	Actualización de la lista de Miembros de las BCR
0.4	01/04/2024	Re branding y formato Alineación con las recomendaciones del EDPB 1/2022 revocando y reemplazando el WP56_Rev01

Frecuencia de Revisión	Este documento será revisado al menos una vez al año o en cuanto haya cambios en las entidades de Webhelp.
Fecha de Expedición	25/05/2018
Dominio	Privacidad
Clasificación	Público
Referencia	EN__GPPriv-01- Normas corporativas vinculantes - Responsable

Anexo 01

List of Concentrix entities bound by the BCR and local privacy email contacts

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
1.	Webhelp Albania Shpk	Rruga Dervish Hima, Stadiumi Air Albania, Qendra e Biznesit, Shkalla BC, nr.B-C, Niveli +3, 1019 Tirana	Albania	privacy@it.webhelp.com
2.	Webhelp Algerie SPA	16bis, cité Bois des Cars 2 16047 Dely Ibrahim	Algeria	privacy@dz.webhelp.com
3.	Webhelp Australia Pty Ltd	Level 16, 201 Elizabeth Street Sydney NSW 2000	Australia	privacy@my.webhelp.com
4.	Webhelp Austria GmbH	Floridsdorfer Haptstrasse 1, 1210 Vienna	Austria	privacy@de.webhelp.com
5.	Webhelp Payment Services Benelux, SA	Avenue Louise, 87 - 1050 Bruxelles	Belgium	privacy@wps.webhelp.com
6.	Webhelp Benin	Immeuble le Jatoba, avenue Jean-Paul II, lot 20, zone résidentielle portuaire; (Nouveau site en cours : Parcelle F G Ilot 40002,quartier Enagnon Akpakpa Cotonou)	Bénin	Privacy@fr.webhelp.com
7.	Webhelp BH d.o.o. Sarajevo	Josipa Stadlera 6, 71000, Sarajevo	Bosnia-Herzegovina	privacy@de.webhelp.com
8.	Services Tech Experience Inovaçao e technologia em relacionamento Ltda	Rua Marechal Deodoro, 314 6th Floor, Sets 601-606, Centro Curitiba, Paraná, 80.010-010	Brazil	protecciondedatos@onelinkbpo.com
9.	Services Assessoria Digital Ltda	Rua Marechal Deodoro 314, 11th floor,Centro Curitiba, Paraná, 80.010-010	Brazil	protecciondedatos@onelinkbpo.com
10.	Webhelp Bulgaria EOOD	Blvd. Totleben, Business-Center Sofia City-West 53-55, 1606, Sofia	Bulgaria	privacy@de.webhelp.com
11.	Les services Webhelp, Inc	880 Rue Roy Est, QC H2L 1E6, Montréal, Quebec	Canada	protecciondedatos@onelinkbpo.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
12.	Webhelp Business Consulting (Shanghai) Co. Ltd	Room 368, Unit 302, No. 211, North Fude Road, Shanghai FTZ	China	privacy@my.webhelp.com
13.	Webhelp (Suzhou) Data Services Co. Ltd	Unit 2605B, 26th Floor, West Tower, China Overseas Fortune Center, No. 9 Suzhou Avenue West, Suzhou Industrial Park	China	privacy@my.webhelp.com
14.	Onelink SAS	Carrera 52 No. 65 91 OF 740 CENTRO COMERCIAL AVENTUR, Medellín	Colombia	Proteccion.dedatos@concentrix.com
15.	Onelink International SAS	Avenida carrera 19 # 28 80 Cc Empresarial Calima Of 401, Bogota	Colombia	Proteccion.dedatos@concentrix.com
16.	Experts Colombia SAS	Carrera 52 No. 65 61, Medellín	Colombia	Proteccion.dedatos@concentrix.com
17.	Getcom Colombia SAS	Diagonal 55 No. 37 41 OF. 601	Colombia	Proteccion.dedatos@concentrix.com
18.	Getcom Servicios SAS	Diagonal 55 Av 37 41 OF 701, Bello	Colombia	Proteccion.dedatos@concentrix.com
19.	Webhelp Enterprise Sales Solutions, s.r.o	Vaclavske namesti 808/66, 11000 Praha, Nové Mesto	Czech Republic	privay@cz.webhelp.com
20.	Webhelp Denmark, AS	Borgmester Christiansens Gade 50, 2, 2500, Copenhagen	Denmark	privacy@nordic.webhelp.com
21.	Webhelp Egypt	plot No. 53, First District, City Center New Cairo, Cairo	Egypt	privacy@eg.webhelp.com
22.	Onelink SA de CV	Avenida Albert Einstein y Bulevar, San Salvador.	El Salvador	Proteccion.dedatos@concentrix.com
23.	Tetel SA de CV	Avenida Albert Einstein y Bulevar, San Salvador.	El Salvador	Proteccion.dedatos@concentrix.com
24.	Getcom International SA de CV	Boulevard Los Próceres, Colonia Palermo Edificio Ex Panades, No.	El Salvador	Proteccion.dedatos@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
		350, Frente a UCA, San Salvador, San Salvador.		
25.	RH-T SA de CV	Avenida Albert Einstein y Bulevar, San Salvador.	El Salvador	Proteccion.dedatos@concentrix.com
26.	Webhelp OÜ	Tartu mnt 63, Tallinn 10115	Estonia	privacy@nordic.webhelp.com
27.	Webhelp Finland, Oy	Palkkatilanportti 1 FI-0240 Helsinki	Finland	privacy@nordic.webhelp.com
28.	GoBeyond Partners, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell , 75017 Paris	France	Privacy@fr.webhelp.com
29.	Webhelp, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	Privacy@fr.webhelp.com
30.	Webhelp Conseil, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	Privacy@fr.webhelp.com
31.	W Automobile Services, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell	France	Privacy@fr.webhelp.com
32.	Webhelp France, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	Privacy@fr.webhelp.com
33.	Webhelp Caen, SAS	1 rue Jean Perrin, 14460 Colombelles	France	Privacy@fr.webhelp.com
34.	Webhelp Compiègne, SAS	ZAC du Parc Tertiaire - 98 impasse Les Terres auprès des Iles, 60610, Compiègne	France	Privacy@fr.webhelp.com
35.	Webhelp Fontenay, SAS	6 Rue de l'Innovation, 85200 Fontenay-le-Comte	France	Privacy@fr.webhelp.com
36.	Marnix French ParentCO, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@webhelp.com
37.	Marnix French TOPCO, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
38.	Marnix, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@webhelp.com
39.	WowHoldCo, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@webhelp.com
40.	Webhelp Gray, SAS	ZAC GRAY SUD 70100 GRAY	France	privacy@fr.webhelp.com
41.	Webhelp Montceau, SAS	16 rue Saint-Eloi, 71300, Montceau les Mines	France	privacy@fr.webhelp.com
42.	Webhelp Vitré, SAS	Parc d'Activité Etrelles, 35370 Etrelles	France	privacy@fr.webhelp.com
43.	Webhelp University France, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@fr.webhelp.com
44.	Webhelp Prestations, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@fr.webhelp.com
45.	Webhelp WTG, SAS	39 rue des métissages 59200 Tourcoing	France	privacy@fr.webhelp.com
46.	Webhelp Medica Customer Expérience	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@webhelpmedica.com ; privacy@patientys.webhelp.com
47.	Patientys, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@webhelpmedica.com ; privacy@patientys.webhelp.com
48.	MED-TO-MED, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@webhelpmedica.com ; privacy@patientys.webhelp.com
49.	WGE (Webhelp Grand-Est, SAS)	Technopole, 9 rue Thomas Edison, Metz	France	privacy@fr.webhelp.com
50.	Webhelp Medica, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@webhelpmedica.com ; privacy@patientys.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
51.	Webhelp SFIA, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@fr.webhelp.com
52.	Webhelp WCS, SAS	12 Rue Alfred Kastler 71530 Fragnes-La Loyere	France	privacy@fr.webhelp.com
53.	Netino, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@fr.webhelp.com
54.	Solvencia, SAS	450 Rue Félix Esclangon, 73290 La Motte-Servolex	France	privacy@wps.webhelp.com
55.	Webhelp O2C Holding, SAS	450 Rue Félix Esclangon, 73290 La Motte-Servolex	France	privacy@wps.webhelp.com
56.	Webhelp KYC Services, SAS	450 Rue Félix Esclangon, 73290 La Motte-Servolex	France	privacy@wps.webhelp.com
57.	Webhelp Payment Services France, SAS	450 Rue Félix Esclangon, 73290 La Motte-Servolex	France	privacy@wps.webhelp.com
58.	Webhelp Payment Services Deutschland, GmbH	Frankfurter Str. 151A, 63303 Dreieich	Germany	privacy@wps.webhelp.com
59.	Webhelp Sun Holding GmbH	Tullnaustrasse 20, 90402, Nuremberg	Germany	privacy@de.webhelp.com
60.	Webhelp Holding Germany GmbH	Tullnaustrasse 20, 90402 Nuremberg	Germany	privacy@de.webhelp.com
61.	Webhelp Deutschland GmbH	Tullnaustrasse 20, 90402 Nuremberg	Germany	privacy@de.webhelp.com
62.	RIGHTHEAD GmbH	Tullnaustrasse 20, 90402 Nuremberg	Germany	privacy@de.webhelp.com
63.	Webhelp Ghana Ltd	SU TOWER, N°18, Castle Road, North Ridge, Accra	Ghana	privacy@fr.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
64.	Webhelp Hellas Business Enterprise Sales SMLTD (MEPE in Greek)	36 Voukourestiou Str 10673 Athens	Greece	privacy@gr.webhelp.com
65.	Onelink Guatemala SA	15 Avenida 17-30 Zona 13, Oficina 201, Guatemala, Guatemala	Guatemala	Proteccion.dedatos@concentrix.com
66.	Onelink Solutions Guatemala SA	15 Avenida 17-40 zona 13, Torre 1, Nivel 1 Edificio Tetra Center, Ciudad de Guatemala	Guatemala	Proteccion.dedatos@concentrix.com
67.	Inversiones Xperts Guatemala SA	15 Avenida 17-40 zona 13, Torre 1, Nivel 1 Edificio Tetra Center, Ciudad de Guatemala	Guatemala	Proteccion.dedatos@concentrix.com
68.	Gobeyond Partners Asia Limited	31/F Tower Two Times Square 1, Matheson St., Causeway Bay, Hong Kong	Hong Kong	privacy@my.webhelp.com
69.	Webhelp India Private Ltd	Corporate Office: Ground Floor, Tower A, SP Infocity, Udyog Vihar, Phase-1, Gurugram-122001, Haryana , India	India	privacy@uk.webhelp.com
70.	SELLBYTEL Marketing Services India Private Ltd	Corporate Office:-Ground Floor, Tower A, SP Infocity, Udyog Vihar, Phase-1, Gurugram-122001, Haryana , India	India	privacy@uk.webhelp.com
71.	Webhelp Israel Ltd	Yigal Alon 94, Alon tower 1 Tel Aviv , Tel-Aviv	Israel	privacy@tr.webhelp.com
72.	Webhelp Payment Services Italia, SRL	Via Gozzano Guido 14 - 20092 Cinisello Balsamo	Italy	privacy@wps.webhelp.com
73.	Webhelp Payment Services France succursale Italie	Via Maurizio Gonzaga n° 7	Italy	privacy@wps.webhelp.com
74.	Webhelp Enterprise Sales Solutions Italy		Italy	privacy@it.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
		Via Torri Bianche, 7, 20871 Vimercate MB, Italy		
75.	Webhelp Cote d'Ivoire	Immeuble PIA, Avenue Abdoulay Fadiga, Plateau Abidjan - 01 BP 7171 ABJ 01	Ivory Coast	privacy@ci.webhelp.com
76.	WH Abidjan Le Workshop	Indenie, 6 rue des Sambas 01 BP 743 ABJ 01, Plateau Abidjan - 01 BP 743 ABJ 01	Ivory Coast	privacy@ci.webhelp.com
77.	Webhelp SAS (succursale Côte d'Ivoire)	Immeuble PIA, Avenue Abdoulay Fadiga, Plateau Abidjan - 01 BP 7171 ABJ 01	Ivory Coast	privacy@ci.webhelp.com
78.	Webhelp Japan KK	Tokyo Club Building 11F, 3-2-6 Kasumigaseki, Chiyoda-ku, Tokyo	Japan	privacy@my.webhelp.com
79.	Webhelp Jordan LLC	Rafiq Al Hariri Ave 1, Amman	Jordan	privacy@jo.webhelp.com
80.	IQ-to-Link shpk	Rr. Ukshin Hoti nr. 121	Kosovo	privacy@de.webhelp.com
81.	Webhelp Kosovo L.L.C.	Rr. Ukshin Hoti nr. 120, 10000, Prishtina	Kosovo	privacy@de.webhelp.com
82.	Webhelp Latvia SIA	Krišjāņa Valdemāra iela 21-18	Latvia	privacy@jo.webhelp.com
83.	Webhelp SIA	Skanstes iela 54A	Latvia	privacy@de.webhelp.com
84.	Webhelp Madagascar, SA (zone franche)	Bâtiment TITAN 2, Zone Galaxy Andraharo, Antananarivo 101	Madagascar	privacy@mg.webhelp.com
85.	Netino Madagascar	Lot II M92 Antsakaviro -Ambodirotra Cua Antananarivo 101 Analamanga	Madagascar	privacy@mg.webhelp.com
86.	Webhelp Malaysia Sdn Bhd	Menara Exchange 106, Level 6, Lingkaran TRX, Jalan Tun Razak, 55188 Kuala Lumpur, Malaysia	Malaysia	privacy@my.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
87.	Onelink Mexico SA de CV	BOULEVARD 300 ENTRE CALLE CDA MEZTISOS - VILLAS DEL REY - CAJEME- OBREGÓN SONORA- MÉXICO, 85136, Ciudad Obregón	Mexico	protecciondedatos@onelinkbpo.com
88.	Onelink Servicios SA de CV	BOULEVARD 300 ENTRE CALLE CDA MEZTISOS - VILLAS DEL REY - CAJEME- OBREGÓN SONORA- MÉXICO, 85136, Ciudad Obregón	Mexico	Proteccion.dedatos@concentrix.com
89.	Webhelp Maroc, SA	43 av Ibn Sina-Agdal-Rabat	Morocco	privacy@ma.webhelp.com
90.	Webhelp SAS Succursale	28 Avenue Allal Ben Abdellah - (Business address: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy@ma.webhelp.com
91.	Webhelp Services, SA	15, Avenue Annakhil (Business address: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy@ma.webhelp.com
92.	Webhelp Contact Center, SA	N°50 BLOC F 11 IMMEUBLE AL FIDIAN I ET IMMEUBLE AL FIDIAN II AVENUE HASSAN I CITE DAKHLA (Business address: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy@ma.webhelp.com
93.	Webhelp Multimedia, SA	6, rue Lalla Nezha, 30000 Fès	Morocco	privacy@ma.webhelp.com
94.	Webhelp GRC, SA	43 Avenue Ibn Sina, 10000 Rabat	Morocco	privacy@ma.webhelp.com
95.	Webhelp Technopolis, SA	Agdal, 25, Rue Oued Al Makhazine (Business adress: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy@ma.webhelp.com
96.	Webhelp University Maroc, SARL	15 av Annakhil, (Business adress: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy@ma.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
97.	Webhelp Agadir, SA	Quartier Industriel, Avenue Hassan II, Immeuble Jaouhara (Business adress: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy@ma.webhelp.com
98.	Webhelp Fès, SA	112 Avenue des FAR Champs de Course ville nouvelle (Business adress: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy@ma.webhelp.com
99.	Webhelp Meknès, SA	Immeuble Angle Rue Badir Al Kobra et Rue Sebou angle rue Badr al Korba, Meknes (Business adress: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy@ma.webhelp.com
100.	Webhelp Marrakech, SA	Quartier Industriel, Avenue Hassan II, Immeuble Jaouhara (Business adress: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy@ma.webhelp.com
101.	Webhelp Afrique	CFC Bridge, lot 58, Rez de Chaussée (Core 1), quartier Casa-Anfa, Hay Hassani - Casablanca	Morocco	privacy@ma.webhelp.com
102.	Webhelp Netherlands Holding, BV	Amersfoortsestraat 28, 3821CB, Amersfoort	Netherlands	privacy@nl.webhelp.com
103.	Customer Contact Management Group, BV	Amersfoortsestraat 28, 3821CB, Amersfoort	Netherlands	privacy@nl.webhelp.com
104.	Webhelp Nederland, BV	Koraalrood 50, 2718SC Zoetermeer	Netherlands	privacy@nl.webhelp.com
105.	Webhelp Enterprise BV	Brammelerstraat 8, 7511JG Enschede	Netherlands	privacy@nl.webhelp.com
106.	Stacelet Holding, BV	Colosseum 42, 7521 PT Enschede	Netherlands	privacy@nl.webhelp.com
107.	Telecats BV	Colosseum 42, 7521 PT Enschede	Netherlands	privacy@nl.webhelp.com
108.	Customer Contact Performance Group B.V.	Herengracht 501 H, 1017B, Amsterdam	Netherlands	privacy@nl.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
109.	CCPG Amsterdam B.V.	Herengracht 501 H, 1017B, Amsterdam	Netherlands	privacy@nl.webhelp.com
110.	CCPG Utrecht B.V.	Herengracht 501 H, 1017B, Amsterdam	Netherlands	privacy@nl.webhelp.com
111.	Xperts Nicaragua SA	Plaza El Sol 2 C. Sur, 1 C. Este, Casa No. 26, Los Robles Managua	Nicaragua	Proteccion.dedatos@concentrix.com
112.	Onelink Nicaragua SA	Barrio Largaespada. B. Largaespada Busto Jose Marti 3 C al Este 1 C al Norte, Managua	Nicaragua	Proteccion.dedatos@concentrix.com
113.	Webhelp Company Severna Makedonija DOOEL Skopje	Bul. VMRO 1, 1000, Skopje, North-Macedonia	North-Macedonia	privacy@de.webhelp.com
114.	Webhelp Norway, AS	Storgata 38, 0182 Oslo	Norway	privacy@nordic.webhelp.com
115.	Webhelp Norway Consulting AS	Storgata 38, 0182 Oslo	Norway	**privacy@nordic.webhelp.com**
116.	Webhelp Perù S.A.C.	Calle Santa Inés Nro. 115, Urbanización Industrial Santa Rosa, distrito Ate, Lima	Peru	protecciondedatos@onelinkbpo.com
117.	BPO Consulting S.A.C.	Jirón Marcos Farfán, n° 3468, Lima	Peru	protecciondedatos@onelinkbpo.com
118.	Webhelp Philippines, Inc.	12th floor, Makati Sky Plaza, 7788 Ayala avenue, Makati City, 1223	Philippines	privacy@my.webhelp.com
119.	Webhelp Poland Sp. z.o.o.	Ul. Taneczna 30, PL 02-829, Warszawa	Poland	privacy@de.webhelp.com
120.	Webhelp Sun Portugal, Unipessoal, Lda	Avenida Professor Cavaco Silva, Tagus Park, Edificio Qualidade, bloco A-2, 2470-296 Porto Salvo, parish of Porto Salvo, Oeiras	Portugal	privacy@pt.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
121.	Webhelp Oeiras, Lda	Avenida Professor Cavaco Silva, Tagus Park, Edificio Qualidade, bloco A-2, Lisboa	Portugal	privacy@pt.webhelp.com
122.	Webhelp Lisbon, Unipessoal, Lda	Avenida D. João II, nº 43, Torre Fernão de Magalhães, 15º Piso, freguesia de Parque das Nações, 1998-025, Lisboa	Portugal	privacy@pt.webhelp.com
123.	Webhelp SAS Succursale em Portugal	Avenida D. João II, nº 43, Torre Fernão de Magalhães, 15º Piso, freguesia de Parque das Nações, 1998-025 Lisboa	Portugal	privacy@pt.webhelp.com
124.	Webhelp Norte, Unipessoal LDA	Av. Mediterrâneo 1, 1990-203 Lisboa, freguesia de Parque das Nações, LIsboa	Portugal	privacy@pt.webhelp.com
125.	Righthead -Empresa de Trabalho Lda	Avenida Professor Cavaco Silva, Tagus Park, Edificio Qualidade, bloco A-2	Portugal	privacy@pt.webhelp.com
126.	WH New Generation Lisbon	Av. Mediterrâneo 1, 1990-203 Lisboa, freguesia de Parque das Nações, 1998-025, Lisboa	Portugal	privacy@pt.webhelp.com
127.	Webhelp SFIA, Sucursal em Portugal	Av. Mediterrâneo 1, 1990-203 Lisboa, freguesia de Parque das Nações, 1998-025, Lisboa	Portugal	privacy@pt.webhelp.com
128.	Webhelp Payment Services Espana, Sucursal em Portugal	Av. Mediterrâneo 1, 1990-203 Lisboa, freguesia de Parque das Nações, 1998-025, Lisboa	Portugal	privacy@wps.webhelp.com
129.	Webhelp Romania SRL	Sector 1, Str. Doctor Iacob Felix, nr. 63-69, et. 2	Romania	privacy@ro.webhelp.com
130.	Pitech Plus SA	Strada Câmpul Pâinii nr.3-5, etajul 3	Romania	privacy@ro.webhelp.com
131.	MindMagnet Plus SRL	Strada Câmpul Pâinii nr.3-5, etajul 3, 400058, Cluj-Napoca	Romania	privacy@ro.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
132.	Webhelp Senegal SAS	Almadies, Pointe des Almadies, en face King Fahd, fahd Palace, 284, TF n°284/NGA Dakar	Senegal	privacy@sn.webhelp.com
133.	Webhelp SAS Succursale Senegal	Almadies, Imm Serenity Pointe des Almadies, en face King Fahd, fahd Palace TF n°284/NGA Dakar	Senegal	privacy@sn.webhelp.com
134.	Webhelp d.o.o Beograd	Makedonska 30, III. Floor, 11000, Beograd	Serbia	privacy@de.webhelp.com
135.	Webhelp Singapore Pte Ltd	9 Raffles Place, #26-01 Republic Plaza, Singapore 048619	Singapore	privacy@my.webhelp.com
136.	Webhelp Slovakia, s.r.o.	Staromestská 3 811 03, Bratislava - mestská časť Staré Mesto	Slovakia Republic	privacy@it.webhelp.com
137.	Webhelp Holding Germany GmbH (Slovenia Branch)	City Centre - Republic square, 1000, Ljubljana	Slovenia	privacy@de.webhelp.com
138.	Concentrix South Africa (Pty) Pty Ltd	19 Ameshoff Street, Braamfontein, Johannesburg, 2001	South-Africa	privacy@uk.webhelp.com
139.	Webhelp SAS, Sucursal en Espana	Plaza Solymar s/n, Edificio Benalmar ,29630 Benalmádena, Málaga	Spain	**privacy@es.webhelp.com**
140.	Direct Medica Iberica S.L.	CL LAGASCA, 95, 28006 MADRID	Spain	privacy@webhelpmedica.com
141.	Webhelp Malaga SLU	Plaza Solymar s/n Edificio WEBHELP, 29630 Benalmádena, Málaga	Spain	privacy@es.webhelp.com
142.	Webhelp Payment Services Espana SA	Calle Vallespir, número 19, módulo 3, planta 1ª de Sant Cugat del Vallès	Spain	privacy@wps.webhelp.fr
143.	Webhelp Spain Business Process Outsourcing S.L.	Avda. Diagonal 197 Barcelona, 08018	Spain	privacy@es.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
144.	Webhelp Spain Holding SLU	Av. Diagonal 97, 12 Barcelona 08018	Spain	privacy@es.webhelp.com
145.	Telenamic NV	Zonnebloemstraat 50, Paramaribo	Suriname	privacy@sr.webhelp.com
146.	Webhelp Sweden AB	Box 4006, 16904 Solna	Sweden	
147.	Webhelp IT Services AB	Box 4006, 16904 Solna	Sweden	privacy@nordic.webhelp.com
148.	Webhelp Schweiz AG	Richtistrasse 5, 8304 Wallisellen	Switzerland	privacy@de.webhelp.com
149.	Webhelp (Thailand) Limited	87/1 Capital Tower All Seasons Place, Unit 1604-6 Floor 16, Pathumwan District, 10330, Bangkok	Thailand	privacy@my.webhelp.com
150.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş. (Webhelp Call Center and Customer Service Joint Stock Company).	Merkez Mh. Ayazma Cd. Papirus Plaza No.37/42	Turkey	privacy@tr.webhelp.com
151.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş. Bingöl Branch (Webhelp Call Center and Customer Service Joint Stock Company).	Bingöl Üniversitesi Fen Edebiyat Fakültesi No:Merkezi Derslik Birimi Bodrum Kat:1 Merkez/Bingöl, 12000 Bingöl	Turkey	privacy@tr.webhelp.com
152.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş.İzmir 2 Branch (Webhelp Call Center and Customer Service Joint Stock Company).	Beyazevler Mahallesi Akçay Cad. No: 99/2, 35410 Gaziemir/ Izmir	Turkey	privacy@tr.webhelp.com
153.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş.Van 2 Branch (Webhelp Call Center and Customer Service Joint Stock Company).	Vali Mithat Bey Mahallesi Cemaller Sk. Roza Aprt Sit. No: 9 A ipekyolu/65100 Van,	Turkey	privacy@tr.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
154.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş.Ümraniye Branch (Webhelp Call Center and Customer Service Joint Stock Company).	Fatih Sultan Mehmet Mahallesi Balkan Cad. Casper Plaza İş Merkezi Apt. No: 47/1 Ümraniye / 34771 Istanbul	Turkey	privacy@tr.webhelp.com
155.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş.Bursa Branch (Webhelp Call Center and Customer Service Joint Stock Company).	Panayır Mahallesi 3. Pınar Cad. No:345 B Osmangazi/ 16250 Bursa	Turkey	privacy@tr.webhelp.com
156.	Bin Çağrı Hizmetleri A.Ş. (Bin Call Services Joint Stock Company)	Bingöl Üniversitesi Fen Edebiyat Fakültesi - Bingöl	Turkey	privacy@tr.webhelp.com
157.	Webhelp İnsan Kaynakları Danışmanlık ve Destek Hizmetleri A.Ş. (Webhelp Human Resources Consultancy and Support Services Joint Stock Company)	Merkez Mh. Ayazma Cd. Papirus Plaza No.37/42, 34406; Kağıthane - Istanbul	Turkey	privacy@tr.webhelp.com
158.	Teknofix Telekomünikasyon ve Bilişim Hizmetleri A.Ş. (Teknofix Telecomunication and Information Services Joint Stock Company)	Aydınevler Mah. Aslanbey Cad. No:1 D:5-6, Küçükyalı, Maltepe, Istanbul	Turkey	privacy@tr.webhelp.com
159.	Teknofix Telekomünikasyon ve Bilişim Hizmetleri A.Ş. Istanbul Kagithane Branch (Teknofix Telecomunication and Information Services Joint Stock Company)	Merkez Mh. Ayazma Cd. Papirus Plaza No.37/42, 3440 Kağıthane - Istanbul	Turkey	privacy@tr.webhelp.com
160.	Teknofix Telekomünikasyon ve Bilişim Hizmetleri A.Ş. Ankara Basinevleri Branch (Teknofix Telecomunication and Information Services Joint Stock Company)	Basınevleri Mah. Yankılar Sok. No:16 Keçiören, Ankara	Turkey	privacy@tr.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
161.	Telecom Service Centres Ltd	11 Central Park Avenue, Central Business Park, Larbert, Falkirk, FK5 4RX,	United-Kingdom	privacy@uk.webhelp.com
162.	Webhelp Payment Services UK Ltd	C/o Civvals Limited, 50 Seymour Street, London W1H 7JG	United-Kingdom	privacy@wps.webhelp.com
163.	Webhelp Medica UK Limited	Building 2, 1 Nunnery Square, S2 5DD, Sheffield	United-Kingdom	privacy@webhelpmedica.com
164.	Webhelp USA Group Inc	1111 Brickell Avenue, Suite 11, FL 33131, Miami	USA	Proteccion.dedatos@concentrix.com
165.	Webhelp USA LLC	1111 Brickell Avenue, Suite 11, FL 33131, Miami	USA	Proteccion.dedatos@concentrix.com
166.	Webhelp US LLC	1111 Brickell Avenue, Suite 11, FL 33131, Miami	USA	Proteccion.dedatos@concentrix.com
167.	Webhelp Logbox USA	110 West 40th Street , Suite 1903 New York, NY 10018	USA	Proteccion.dedatos@concentrix.com
168.	Webhelp Americas LLC	80 SW 8TH ST, SUITE 2900, FL 33130, Miami	USA	Proteccion.dedatos@concentrix.com
169.	Webhelp California Inc.	200 Madison Avenue, Suite, 1901, NY 10016,New York	USA	Proteccion.dedatos@concentrix.com

Anexo 2
Definiciones para las BCR y Procedimientos

“Legislación aplicable sobre protección de datos”	Significa, en el siguiente orden de prevalencia, (i) el Reglamento Europeo 2016/679 relativo al Tratamiento de Datos Personales a partir de su fecha de aplicación («RGPD»), (ii) las leyes y reglamentos nacionales de los Estados miembros de la UE relativos al Tratamiento de Datos Personales y que implementan el RGPD y (iii) cualquier normatividad relativa al Tratamiento de Datos Personales aplicable durante la vigencia de la presente Política de Privacidad.
“Norma Corporativa Vinculante” o BCR	Hace referencia a las políticas y procedimientos de protección de Datos Personales a los que se adhieren los Miembros de las BCR para transferencias o un conjunto de transferencias de Datos Personales a un Responsable o Encargado de Datos en uno o más países terceros dentro del grupo Concentrix.
“Miembro de las BCR”	Se refiere a cualquier filial del grupo Concentrix que haya firmado y esté obligada por las BCR-C y/o las BCR-P y que, como tal, se haya comprometido a cumplir dichas BCR; los miembros de las BCR se enumeran en el Anexo 01 de dichas BCR-C y BCR-P.
“Cliente corporativo”	Significa cualquier tercero, que contrate con Concentrix y actúe como controlador de datos, cuyos datos personales sean tratados por un miembro del BCR que actúe como Responsable de los datos de acuerdo con sus instrucciones documentadas.
“AS Competente” o “Autoridad de supervisión competente”	Autoridad de Control del EEE para el exportador de datos
“Datos” o “Información”	Se refiere a cualquier tipo de información accesible individualmente por medios electrónicos o de otro tipo como registros, datos personales, documentos u otros materiales.
“Base de datos”	Es una colección de obras, datos, información u otros materiales independientes dispuestos de forma sistemática o metódica y accesibles individualmente por medios electrónicos o de otro tipo.
"Exportador de datos"	Hace referencia al Responsable o Encargado del Tratamiento que transfiere los Datos Personales a un país tercero no perteneciente al EEE

“Importador de datos”	Se refiere al Responsable o Encargado del tratamiento que recibe los datos personales.
“Responsable de los datos” o “Responsable”	Significa la persona física o jurídica, autoridad pública, agencia u otro organismo que, solo o conjuntamente con otros, determine los fines y los medios del Tratamiento de Datos Personales.
“Encargado de los datos” o “Encargado”	Significa una persona física o jurídica, autoridad pública, agencia u otro organismo que procesa Datos Personales en nombre del Responsable del Tratamiento.
“Titular de los datos”	Significa cualquier persona física que pueda ser identificada, directa o indirectamente, mediante medios que probablemente puedan ser utilizados por cualquier persona física o jurídica, en particular mediante la referencia a un identificador como un nombre, un número de identificación, datos de ubicación, un identificador en línea o a uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de esa persona.
“Dispositivo”	Significa cualquier objeto programable que pueda realizar automáticamente una secuencia de cálculos u otras operaciones sobre datos una vez que ha sido programado, ya sea directamente o indirectamente, para esa tarea. Cualquier aparato electrónico adaptado para mostrar la información en un formato legible. Los dispositivos incluyen, pero no se limitan a, computadoras, teléfonos inteligentes, tabletas, laptops, servidores, redes, plataformas de telefonía, etc.
EEE	Significa el Espacio Económico Europeo. Los países que forman parte del EEE son los Estados miembros de la UE, así como Islandia, Liechtenstein y Noruega.
“Autoridad de Supervisión del EEE”	Significa una autoridad independiente de protección de datos pública que está establecida en un Estado miembro del EEE.

“Cifrado”	Significa un proceso para ofuscar datos transformando los datos en una forma en la que hay una baja probabilidad de asignarles un significado o hacerlos legibles, excepto cuando se utilizan en conjunto con un proceso confidencial o una clave para decodificarlos. Tal proceso podría ser, pero no se limita a, una función matemática o un proceso algorítmico.
“Administrador de la información”	Significa la persona física dentro de la organización de Concentrix que, sola o conjuntamente con otros, procesa o manipula la información de acuerdo con las necesidades, los objetivos, los fines y las reglas del Propietario de la Información.
“Propietario de la información”	Significa la persona física dentro de la organización de Concentrix que, sola o conjuntamente con otros, determina las necesidades, el objetivo, los fines y las reglas de un proyecto que incluya el procesamiento de la información.
“Acuerdo Intragrupal de Transferencia de Datos”	Significa el acuerdo intra-grupo que comprende el BCR-C y el BCR-P como anexos, que todos los Miembros del BCR están obligados a ejecutar para estar vinculados por el BCR-C y el BCR-P.
“Sistemas de Información”	Significa cualquier Dispositivo utilizado directa o indirectamente por un Usuario u otro Dispositivo para procesar Información, incluyendo, pero no limitándose a, la recopilación, grabación, organización, estructuración, almacenamiento, adaptación, alteración, recuperación, consulta, uso, divulgación por transmisión, difusión u otra forma de poner a disposición, alineación o combinación, restricción, eliminación o destrucción de Datos.
“Líder Local en Privacidad”	Significa la persona que es el principal punto de contacto del Oficial de Privacidad de datos (DPO por sus siglas en inglés) y que se encarga de los asuntos de protección de datos dentro de cada Miembro de las BCR.
“Software Malicioso”	Significa software que, al ser introducido, afecta negativamente la función prevista del software o

	hardware. Esto puede incluir, pero no se limita a, virus, malware, troyanos, ransomware, etc.
“Redes”	Significa la conectividad física o lógica que permite que dos o más dispositivos se comuniquen.
“Contraseña” o “Frase de Contraseña”	Significa una cadena de caracteres o cualquier otro medio lógico o físico utilizado en conjunto con una Identidad de Usuario durante un proceso de autenticación para probar la identidad de un Usuario y/o otorgar acceso a cierta Información.
“Datos Personales”	Significa cualquier información relacionada con una persona natural identificada o identificable (un Titular de Datos); una persona natural identificable es aquella que puede ser identificada, directa o indirectamente, en particular mediante la referencia a un identificador como un nombre, un número de identificación, datos de ubicación, un identificador en línea o a uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de esa persona natural. Los Datos Personales incluyen Datos Personales Sensibles.
“Violación de Datos Personales”	Significa una violación de la seguridad que conduce de manera accidental o ilegal a la destrucción, pérdida, alteración, divulgación no autorizada o acceso a Datos Personales, ya sea transmitidos, almacenados o de otro modo procesados.
“Comité de Privacidad”	Significa el comité interno de la junta que apoya al Oficial Global de Privacidad de Datos.
“Tratamiento” o “Procesamiento”	Significa cualquier operación o conjunto de operaciones realizadas sobre Datos Personales o sobre conjuntos de Datos Personales, ya sea por medios automatizados o no, tales como recopilación, grabación, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación por transmisión, difusión o de otro modo puesta a disposición, alineación o combinación, restricción, eliminación o destrucción.
“Seudonimización”	Significa el Tratamiento de Datos Personales de tal manera que los Datos Personales ya no puedan atribuirse a un Titular de Datos específico sin el uso de información adicional, siempre que dicha información adicional se mantenga por separado y esté sujeta a medidas técnicas y organizativas para

	garantizar que los Datos Personales no se atribuyan a una persona natural identificada o identificable.
“Riesgo”	Significa un escenario que describe un evento y sus consecuencias, estimadas en términos de severidad y probabilidad.
“Gestión de Riesgos”	Significa las actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.
“Incidente de Seguridad”	Significa acceso o intente de acceso no autorizado al uso, divulgación, modificación o destrucción de Información, o la interferencia con las operaciones del sistema en el Sistema de Información.
“Datos Personales Sensibles”	Significa categorías especiales de Datos Personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y libertades fundamentales, requiriendo que dichos Datos Personales merezcan una protección específica, ya que el contexto de su Tratamiento podría crear riesgos significativos para los derechos y libertades fundamentales. Estos datos incluyen, por ejemplo, Datos Personales que revelan el origen racial o étnico, la opinión política, las creencias religiosas o filosóficas, o la afiliación sindical, así como el Tratamiento de datos genéticos, datos biométricos con el fin de identificar de manera única a una persona física, datos sobre la salud, y datos sobre la orientación sexual de una persona natural.
“Acuerdo de Servicios”	Significa el acuerdo celebrado entre una filial de Concentrix y su Cliente, en virtud del cual dicha filial de Concentrix proporciona servicios a su Cliente.
“Sub-Encargado”	Significa la entidad contratada por un Encargado de Datos para llevar a cabo actividades de procesamiento específicas en nombre del Responsable de Datos, y que está sujeta a las mismas obligaciones de protección de datos establecidas en el contrato u otro acto legal entre el Responsable de Datos y el Encargado de Datos.
“Software” o “Aplicación”	Significa cualquier código, instrucción, programa o rutina que permita la manipulación de Datos de manera directa o remota a través de cualquier medio, e incluye API, shells de comandos, etc.
“Transferencia de Datos Personales”	Significa el Tratamiento, la transferencia material o el acceso remoto a Datos Personales desde entidades establecidas fuera del Espacio Económico Europeo (EEE).

“Usuario”	Significa todos los empleados de Concentrix, terceros, empleados de terceros, contratistas, empleados de contratistas y otras personas cuya conducta y funciones permiten el acceso a los Sistemas de Información de Concentrix.
“Concentrix” o “Grupo Concentrix”	Para el BCR y los Procedimientos relacionados, Concentrix se referirá a Webhelp SAS y a todas las entidades enumeradas en la Lista de entidades vinculadas por el BCR y que, por lo tanto, son Miembros de las BCR

Apéndice 5

Procedimiento del Responsable para el manejo de solicitudes y quejas de los Titulares de Datos

Tabla de Contenidos

1. Introducción

La adopción de las BCR (por sus siglas en inglés) y el compromiso de los Miembros de las BCR de cumplir con ellas demuestra el compromiso de los Miembros de las BCR de proporcionar un alto nivel de protección a los Datos Personales que procesan. Los Miembros de las BCR se comprometen a llevar a cabo sus actividades de acuerdo con la Legislación de Protección de Datos Aplicable, incluyendo el Reglamento Europeo 2016/679 relativo al procesamiento de Datos Personales a partir de su fecha de aplicación, y cualquier normativa relacionada con el procesamiento de Datos Personales aplicable durante la vigencia de la Política de Privacidad. En consecuencia, Concentrix ha implementado el siguiente procedimiento.

Los términos en mayúsculas utilizados en este documento tendrán el mismo significado que el especificado en el Apéndice 2 – Definiciones de Privacidad para las BCR y Procedimiento de las BCR.

2. Objetivos del Procedimiento

Los Titulares de los datos, incluyendo empleados Miembros de las BCR, son dotados de derechos específicos con respecto al tratamiento de sus Datos Personales, tal como se define en la Sección 7 de las BCR.

Cuando se ejerce como responsable de los datos, los Miembros de las BCR van a asegurarse que cualquier solicitud o reclamo del titular de los datos con relación al ejercicio de sus derechos ("**Solicitudes**") será atendido en un tiempo efectivo definido acá, en aras de cumplir con las BCR y la Legislación Aplicable a la Protección de Datos.

Este documento describe como los Miembros de las BCR deberán manejar una solicitud de un Titular de Datos cuando un Miembro de las BCR actúa como Responsable de los datos (Grupos de interés, pasos y líneas de tiempo). Cuando la solicitud es recibida del titular de los datos y esos datos personales son procesados por un miembro Concentrix BCR en representación de uno de los clientes de un miembro de Concentrix BCR, todas las solicitudes deberán ser manejadas de acuerdo con el procedimiento especificado y definido en **Apéndice 06 – Procedimientos para el manejo de solicitudes del titular de los datos donde Concentrix actúa como encargado de los datos.**

3. Procedimientos

Como un paso preliminar, los miembros de las BCR deberán expresamente informar a los titulares de los datos que pueden ejercer sus derechos de acuerdo con las provisiones del artículo 7 de las BCR.

3.1 Contacto y confirmación de recibido de la solicitud

3.1.1 Procedimiento Estándar

Miembros de las BCR deberán también especificar como dichos derechos pueden ser ejercidos. Para este propósito, los Miembros BCR deberán proveer al Titular de los datos medios accesibles para el ejercicio de sus derechos y, en particular un único contacto electrónico dedicado para ser usado sin distinción del país donde el Titular de los datos este localizado. Por esto, cualquier solicitud como parte de este proceso podría ser enviado directamente a la siguiente dirección: dpo@concentrix.com y protección.dedatos@concentrix.com – correos electrónicos locales pueden ser usados para tomar en cuenta alguna especificación local, como el lenguaje.

Al recibir un Solicitud, el Oficial de Privacidad ("**DPO**") del grupo, o cualquier otro individuo o entidad, interna o externa, citada por el DPO para el proceso del manejo de las siguientes responsabilidades, deberá confirmar recibido a no más tardar los 3 días laborales luego de que dicha solicitud sea recibida.

3.1.2 Excepción

En el evento de un reclamo recibido por parte de un titular de los datos mediante un canal distinto al descrito anteriormente, el miembro BCR u otro órgano que reciba el reclamo deberá inmediatamente al ser notificados, contactar al DPO y (1) servicios postales internos, (2) Líderes de Privacidad Local, (3) Referente de Negocios de la Privacidad, y (4) departamentos RH de dicho procedimiento.

El Oficial de Privacidad del Grupo, o cualquier otro individuo o entidad, interna o externa, mencionada por el DPO para el propósito del manejo de las siguientes responsabilidades deberá hacer acuso de recibido del asunto por escrito en los 2 días laborales siguientes desde la notificación de la función.

3.2 Recolección de Información

Antes del envió de una solicitud interna, el Oficial de Privacidad del Grupo, o cualquier otro individuo o entidad, interna o externa, designado por el DPO para el propósito del manejo de las siguientes responsabilidades, debe (1) asegurarse que se tiene la información mínima requerida por parte del Titular de los Datos para especificar sus solicitudes (2), de ser considerado necesario, obtener tanta información como sea posible para aprobar que la solicitud sea manejada adecuadamente.

Como mínimo, y en la medida de lo posible, deberá obtenerse la siguiente información ("**Información Mínima**"):

- Primer nombre y apellidos de los titulares de los datos; y

- Cuando sea legalmente permitido/necesario, copia de la identificación del Titular de los Datos o cualquier otro documento requerido como prueba de identidad; y
- Detalles de contacto para ser usados al localizar de regreso al Titular de los Datos; y
- Los Datos Personales afectados por la Solicitud y el objeto de la misma; y
- Fecha de cuando los Datos Personales fueron inicialmente recibidos; y
- Tipo de derecho que el Titular de los Datos desea ejercer (por favor indicar ya sea acceso, eliminación, bloqueo, o corrección).

De ser considerado necesario, miembros BCE deberán obtener la siguiente información:

- Miembro BCR que inicialmente recolectó los Datos Personales; y
- Categoría del tratamiento con relación al cual el titular de los datos está iniciando su solicitud;
- Cualquier detalle relevante a la solicitud.

Con tal de obtener la información necesaria, el miembro BCR puede invitar al Titular de los Datos, quien no ha especificado suficiente información en su correo, para completar a detalle el documento de cuestionario, con campos de edición libre, o cualquier otro medio iniciado por Concentrix para facilitar la recolección de información requerida del Titular de los Datos. (Por ejemplo: campos pre-completados en el documento, opciones disponibles mediante cuadros de selección, etc.) Significa autorizar la recolección de datos, en mínimo, indicando (1) si la respuesta es mandatoria o no y (2) las consecuencias si no se brinda respuesta.

3.3 Análisis de la solicitud

El Oficial de Privacidad de Datos (DPO), o cualquier otro individuo o entidad, interna o externa, designada por el DPO para el propósito del manejo de las siguientes responsabilidades, deberá determinar si han obtenido la información mínima para procesar la solicitud.

Con base en la información solicitada y obtenida, el DPO deberá determinar la solicitud. Si considera que la solicitud es razonable y legitima (opuesto a una solicitud sin pruebas de identidad del titular de los datos, una demanda excesiva que resulte en solicitudes repetitivas, solicitudes de datos ya eliminados de acuerdo con el periodo de retención, solicitudes a nombre de otros, datos futuros de oficios, etc.) entonces:

El DPO deberá (i) documentar cualquier solicitud recibida y (ii) hacer el análisis relevante de la solicitud. Para analizar correctamente la solicitud, el DPO o cualquier otro individuo o entidad, interna o externa, designada por el DPO con el propósito de manejar las responsabilidades anteriores podría necesitar dar respuesta a las siguientes preguntas:

- ¿Cuál es la naturaleza de la solicitud? (acceso, eliminación, oposición, correción, portabilidad)
- ¿Tengo la información necesaria para identificar al Titular de los Datos?;
- ¿Tengo información necesaria con respecto al alcance de la solicitud? (geográfico y parámetros materiales);
- ¿Tiene el Titular de los Datos en su posesión los datos solicitados o fácil acceso a ellos (por ejemplo, mediante los sistemas de Concentrix)?;

- ¿La solicitud incluye información que no está en un formato claro para los Titulares de los Datos? En caso de que así sea, asegurarse que se expliquen los códigos para que la información sea comprendida;
- ¿Está la solicitud del Titular de los Datos basada en un interés legítimo?;
- ¿Es técnicamente posible atender la solicitud del Titular de los Datos (particularmente el volumen de datos en cuestión)?;
- ¿Hay terceros involucrados en el tratamiento de Datos Personales del Titular de los Datos dentro del ámbito de la solicitud?;
- ¿Podría el manejo de la solicitud implicar que Datos Personales de terceros sean comunicados al Titular de los Datos? En caso de que sí, ¿es posible únicamente extraer Datos Personales del solicitante, con esfuerzos razonables y sin riesgo para los Datos Personales de terceros? En caso de que no, estos Datos Personales no pueden ser comunicados al Titular de los Datos.

3.4 Identificación del tipo de respuesta

En este apartado, uno puede contemplar tres casos distintos:

3.4.1 Caso 1

Cuando la información dada por el Titular de los Datos **no es suficiente** para manejar la solicitud, el DPO, o cualquier otro individuo o entidad, interna o externa designada por el DPO con el propósito del manejo de las siguientes responsabilidades, deberá enviar una solicitud al Titular de los Datos para información adicional a no más tardar 10 días laborales luego de recibir la solicitud.

Cuando la solicitud sea demasiado compleja y sujeta a conformidad con cualquier requerimiento legal, la línea de tiempo de respuesta podría ser extendida hasta los 2 meses, sujeto a documentación del análisis de complejidad por el DPO.

3.4.2 Caso 2

Cuando el DPO considere en su análisis inicial, que la solicitud podría **no ser legítima como se describe en la sección 3.7**, no debería inmediatamente concluir el caso. El Oficial de Privacidad del Grupo, o cualquier otro individuo o entidad, interna o externa, designada por el DPO con el propósito del manejo de las siguientes responsabilidades, deberá responder al Titular de los Datos en los próximos 10 días laborales luego de recibir la solicitud, requiriendo al Titular de los Datos proveer más explicaciones del porqué el Titular de los Datos tiene la intención de ejercer esos derechos.

Cuando sea necesario, el DPO podría informar a grupos de interés relevantes en un nivel local y al Líder Local de Privacidad.

Una vez recibida una justificación adicional con respecto a la legitimidad de la solicitud, el DPO, o el Líder Local de la Privacidad debe, en los próximos 15 días laborales luego de recibida la información del titular de los datos, (1) asegurar que responde a la solicitud, o (2) cuando él o ella considere durante el primer análisis que la solicitud mencionada por el Titular de los Datos no es legítima, se documente porqué se considera la solicitud ilegítima y responda al Titular de los Datos.

La guía para el análisis de legitimidad de la solicitud es dada anteriormente para dicho procedimiento. La respuesta deberá incluir la razón por la cual no toma

acción y la posibilidad del Titular de los Datos para albergar un reclamo con una autoridad protectora de datos y la búsqueda de un remedio judicial.

Cuando el DPO o algún miembro relevante de la cadena de privacidad (es decir, Líder de Privacidad Regional y/o Local) considere que, basado en los elementos adicionales, la solicitud pueda ser manejada, deberá asegurarse de responder al Titular de los Datos en los anteriormente mencionados 15 días laborales. Cuando la solicitud sea muy compleja y sujeta a normativa con cualquier requerimiento legal, la línea de tiempo de respuesta podría ser extendida hasta 2 meses, sujeta a documentación del análisis de complejidad por el DPO.

3.4.3 Caso 3

Cuando la información dada por el Titular de los Datos es suficiente, el DPO deberá asegurar que se responda a la solicitud sin atraso y máximo a **1 mes desde el recibido de la solicitud.**

Por favor tomar en cuenta que en cualquier caso la respuesta al titular de los datos debe ocurrir en 1 mes a más tardar luego de recibir la solicitud (excepto en circunstancias específicas y limitadas ya detalladas en este documento).

3.5 Provisiones locales mandatorias

El Líder Local de la Privacidad, de no ser designado directamente por el DPO para el proceso del manejo de las respuestas a las solicitudes recibidas por un miembro BCR, deberá estar listo para cooperar con el DPO proveyendo a este último con cualquier información relevante con relación al tema. El DPO deberá entonces guiar en cómo manejar el caso, considerando las circunstancias locales, en los 7 días laborales luego de recibir la información por parte del Líder Local de Privacidad.

3.6 Proceso de escalación

Cuando el Titular de los Datos no esté satisfecho con la respuesta inicial dada por el Líder Local de Privacidad o el DPO, y resultado del manejo del procedimiento descrito anteriormente, dicho Titular de los Datos estará autorizado en cualquier caso a inmediatamente solicitar que su solicitud sea re-examinada.

El Titular de los Datos deberá proveer al miembro BCR una explicación detallada de las provisiones insatisfactorias de la solución previamente brindada. El DPO informará al Comité de Privacidad dicha solicitud, y permitirá al Comité de Privacidad el proceder al análisis de dicha solicitud.

Tomando en consideración el análisis dado por el Comité de Privacidad, y sin revelar dicho análisis al Titular de los Datos, el DPO, deberá tomar no más de 2 meses desde el recibido de la solicitud para reexaminación para determinar cómo será manejado e informado al Titular de los Datos por escrito propiamente.

3.7 Rechazo de una solicitud

Aunque los Miembros de las BCR están comprometidos al manejo eficiente de solicitudes de los Titulares de Datos, bajo ciertas circunstancias, los Miembros de las BCR podrían estar autorizados a no aceptar solicitudes de los Titulares de Datos.

Miembros de las BCR tienen el derecho de rechazar una solicitud de un Titular de Datos, cuando al acceder dicha solicitud podría real o potencialmente significar que la siguiente información sea compartida con el Titular de los Datos:

- información amparada por privilegio legal;
- información que un miembro BCR está legalmente prohibido a comunicar;
- información que Miembros de las BCR estén procesando durante el curso de una investigación activa o procedimiento de litigación pendiente.

Cuando información/Datos Personales acerca de otros Titulares de Datos sean visibles, estos datos podrían ser redactados antes de ser compartidos con el Titular de los Datos.

Adicionalmente, cuando el titular de los datos objete más tratamiento de sus Datos Personales y/o solicite por eliminación de sus Datos Personales, los Miembros de las BCR podrían denegar dicha solicitud cuando haya obligación legal sobre o acerca de algún interés prioritario legítimo para que un miembro BCR retenga datos personales. Esto debería ser analizado caso a caso y documentado apropiadamente.

En cualquier caso, si una solicitud o reclamo del Titular de los Datos es denegada por un miembro BCR o la respuesta no sea satisfactoria, el Titular de los Datos puede contactar al DPO y / o puede directamente presentar un reclamo a su Órgano de Vigilancia competente.

3.8 Comunicación con el Titular de los Datos

Cuando se comunique con el titular de los datos, los Miembros de las BCR deberán cooperar con el Titular de los Datos y atender cualquier solicitud a tiempo. Toda la comunicación debe ser proveída utilizando un lenguaje claro y sencillo, en un formato comprensible, conciso, y de fácil acceso.

La información a ser dada al Titular de los Datos debe ser acertada y limitada a (i) lo que el titular de los datos ha solicitado y (ii) la lista de información que podría ser brindada por el Responsable de los Datos de acuerdo con la Legislación Aplicable de la Protección de Datos.

Como regla general, los Miembros de las BCR no deberán aplicar cargos para solicitudes razonables de los Titulares de los Datos. Sin embargo, bajo ciertas circunstancias, particularmente cuando el manejo de la solicitud pueda requerir esfuerzos adicionales por parte de un miembro BCR, cargos razonables, sujetos a un máximo nacional según las leyes aplicables, podrían ser aplicable dado que el Titular de los Datos estará informado de dichos cargos previamente.

-

Preguntas acerca de este procedimiento o conocimiento de alguna violación o potencial violación al procedimiento debe ser reportado directamente al Oficial de Privacidad del Grupo.

Apéndice 6
Procedimiento del Encargado para el manejo de solicitudes y quejas de los Titulares de Datos

Tabla de contenidos

1. Introducción

La adopción de las BCR (por sus siglas en inglés) y el compromiso de los Miembros de las BCR de cumplir con ellas demuestra el compromiso de los Miembros de las BCR de proporcionar un alto nivel de protección a los Datos Personales que procesan. Los Miembros de las BCR se comprometen a llevar a cabo sus actividades de acuerdo con la Legislación de Protección de Datos Aplicable, incluyendo el Reglamento Europeo 2016/679 relativo al procesamiento de Datos Personales a partir de su fecha de aplicación, y cualquier normativa relacionada con el procesamiento de Datos Personales aplicable durante la vigencia de la Política de

Privacidad. En consecuencia, Concentrix ha implementado el siguiente procedimiento.

Los términos en mayúsculas utilizados en este documento tendrán el mismo significado que el especificado en el Apéndice 2 – Definiciones de Privacidad para las BCR y Procedimiento de las BCR.

2. Objetivos del Procedimiento

Los Titulares de los datos, incluyendo empleados Miembros de las BCR, son dotados de derechos específicos con respecto al tratamiento de sus Datos Personales, tal como se define en la Sección 7 de las BCR.

Cuando se ejerce como Encargado de los Datos, los Miembros de las BCR van a asegurarse que cualquier solicitud o reclamo del Titular de los Datos con relación al ejercicio de sus derechos ("**Solicitudes**") será atendido en un tiempo efectivo definido acá, en aras de cumplir con las BCR y la Legislación Aplicable a la Protección de Datos. Sin embargo, esto solo se aplicará cuando los Miembros de las BCR realmente procesen la información solicitada.

Este documento describe como los miembros de las BCR deberán manejar una solicitud de un Titular de Datos cuando un miembro de las BCR actúa como Encargado de los datos (Grupos de interés, pasos y líneas de tiempo). Cuando la solicitud es recibida del Titular de los Datos y esos Datos Personales son procesados por un Miembro de las BCR solo en su propio nombre, como Responsable de Datos, deberán ser manejadas de acuerdo con el procedimiento específicamente definido Políticas y **procedimiento 05 - Procedimiento a seguir por el Responsable para el manejo de solicitudes y quejas de los Titulares de Datos.** En la mayoría de los casos, una solicitud de un individuo (por ejemplo, un empleado del cliente, usuario final del cliente) se encontrará en la siguiente situación:

Las condiciones de procesamiento no cumplen con la Legislación Aplicable de Protección de Datos (por ejemplo, los datos de salud no se utilizan, almacenan y/o cifran de acuerdo con la legislación sanitaria local aplicable);

- El individuo desea ejercer sus derechos de privacidad de acuerdo con la Legislación Aplicable de Protección de Datos, tales como:
  - Acceder a los Datos Personales relacionados con él/ella y procesados por los Miembros de las BCR en nombre del Cliente con el que han establecido una relación;
  - Obtener la rectificación, eliminación o suspensión de cualquier Dato Personal inexacto o incompleto relacionado con él/ella, o que ya no se procese para un propósito válido o apropiado;
  - Oponerse al procesamiento de sus Datos Personales en cualquier momento, a menos que dicho procesamiento sea requerido por la legislación aplicable, siempre que el individuo demuestre que tiene una base legítima para oponerse en relación con su situación particular; y
  - Recibir sus Datos Personales en un formato estructurado, de uso común y legible por máquina.

Incluso si dicho individuo no tiene una relación directa con Concentrix, puede haber casos en los que los Miembros de las BCR reciban una Solicitud directamente del individuo y/o sean solicitados por el Cliente para manejar la Solicitud en su nombre. **Los Miembros de las BCR deberán, en cualquier caso, referirse al**

compromiso con el Cliente para verificar si se aplican condiciones específicas para el manejo de la Solicitud (por ejemplo, prohibición de comunicarse directamente con los Titulares de Datos, etc.).

Como consecuencia, los costos y los impactos técnicos de la Solicitud deben ser anticipados y abordados al inicio de cada compromiso.

3. Procedimientos

Concentrix, actuando como Encargado, no es responsable de informar a los Titulares de Datos sobre sus derechos en relación con los Datos Personales. A menos que las leyes y regulaciones aplicables dispongan lo contrario, dichas obligaciones son responsabilidad del Encargado de Datos. No obstante lo anterior, los Miembros de las BCR se comprometen a proporcionar garantías suficientes mediante la implementación de medidas técnicas y organizativas apropiadas de tal manera que el Tratamiento de Datos Personales en nombre del Encargado de Datos cumpla con los requisitos aplicables y garantice la protección de los derechos del Titular de Datos. Por lo tanto, los procedimientos a continuación se aplican cuando Concentrix actúa como Responsable de Datos en nombre de un Encargado de Datos.

Dado que no se puede excluir formalmente que un Titular de Datos envíe su Solicitud directamente a un Miembro de las BCR, deben considerarse dos casos diferentes.

3.1. Solicitud recibida directamente por un Miembro de las BCR

3.1.1. Comunicación interna

Cualquier Solicitud relacionada con Datos Personales que Concentrix procese como Encargado de Datos (por ejemplo, en nombre de sus Clientes) recibida por un empleado o equipo de trabajo de un Miembro de las BCR debe ser comunicada de **inmediato** al Líder de Privacidad Local o al Referente de Privacidad del Negocio. El Referente de Privacidad del Negocio deberá informar de inmediato al Líder de Privacidad Local.

Como medida de eficiencia, dicha Solicitud también puede ser comunicada al DPO a través del siguiente correo electrónico:

dpo@concentrix.com

El DPO asignará la Solicitud al Líder de Privacidad Local correspondiente a más tardar en 1 día hábil después de su recepción.

La información proporcionada por el empleado o equipo de trabajo de Concentrix debe especificar al menos la siguiente información:

Nombre del gerente local encargado de la cuenta del Cliente;
Copia de la Solicitud; y
Nombre del Cliente con el que está relacionado el Sujeto de Datos.

El Referente de Privacidad del Negocio deberá informar de inmediato a su Líder de Privacidad Local.

3.1.2. Transferencia de la Solicitud al Cliente

Una vez que reciba dicha Solicitud, el Líder de Privacidad Local redactará una comunicación al Cliente sobre la Solicitud. Dicha comunicación deberá (1) ser enviada por el Líder de Privacidad Local al Cliente, en cooperación con el gerente local encargado de la relación con el Cliente; y (2) a más tardar 2 días hábiles después de recibir la Solicitud. El Líder de Privacidad Local también informará al DPO que la Solicitud ha sido transferida al Cliente.

3.1.3. Asistencia del Miembro de las BCR al Cliente

Al mismo tiempo, el Líder de Privacidad Local, con el apoyo de los equipos de operaciones y gestión de cuentas, deberá evaluar y verificar si Concentrix realmente procesa los Datos Personales del Titular de Datos que presenta la Solicitud.

No se proporcionará respuesta sin las instrucciones del Cliente.

En caso de que el Cliente permita a los Miembros de las BCR manejar la Solicitud en su nombre, el Líder Local del Miembro de las BCR deberá determinar con el Cliente si el Cliente mismo o el Miembro de las BCR deberá acusar recibo de la Solicitud e informar al Titular de Datos sobre el papel del Miembro de las BCR en el procesamiento de su Solicitud.

A menos que el Cliente indique lo contrario de manera expresa, los Miembros de las BCR no deberán contactar al Sujeto de Datos durante todo el procedimiento.

3.2. Solicitud enviada por el Responsable de Datos a un Miembro de las BCR

3.2.1. Comunicación interna

Cualquier Solicitud relacionada con Datos Personales que Concentrix procese como Encargado (por ejemplo, en nombre de sus Clientes) recibida por un empleado o equipo de trabajo de un Cliente debe ser comunicada **de inmediato** al Líder de Privacidad Local o al Referente de Privacidad del Negocio. El Referente de Privacidad del Negocio deberá informar de inmediato a su Líder de Privacidad Local.

Cuando un Cliente envíe a un Miembro de las BCR una Solicitud del Titular de los Datos sobre el procesamiento de sus Datos Personales para que la maneje, el Miembro de las BCR deberá acusar recibo de la misma al Cliente a más tardar 2 días hábiles después de recibir dicha Solicitud.

A más tardar 5 días hábiles después de la recepción de la Solicitud, el Miembro de las BCR deberá verificar el grado en que puede atender y manejar la Solicitud.

3.3. Análisis de la solicitud

Tras la recepción de una Solicitud, ya sea directamente del Titular de los Datos o del Cliente, y sujeto a las disposiciones y pasos descritos en este Procedimiento, el Líder de Privacidad Local, o cualquier otra persona o entidad, interna o externa, designada por el Líder de Privacidad Local para el propósito de gestionar las siguientes tareas, deberá asegurarse y verificar que tiene toda la información

necesaria del Cliente y del Titular de los Datos para atender su Solicitud, en particular:

¿La información proporcionada permite al Miembro de las BCR identificar al Titular de los Datos? (es decir, nombre y apellido del Titular de los Datos);
Descripción del contexto en el que se recolectaron los Datos Personales (si es posible)
¿Está autorizado el Miembro de las BCR para manejar la Solicitud en nombre del Cliente?
¿Cuál es la naturaleza de la Solicitud? (acceso, eliminación, oposición, rectificación, portabilidad)
¿Considera el Cliente que la Solicitud del Titular de los Datos es razonable?
¿Es técnicamente posible atender la Solicitud del Titular de los Datos (considerando en particular el volumen de datos en cuestión)?
¿Tiene el Miembro de las BCR suficiente información sobre el alcance de la Solicitud? (alcance geográfico y material, fecha aproximada en que se recolectaron los datos;)
¿Tiene el Titular de los Datos en su posesión los datos solicitados o fácil acceso a ellos?
¿La solicitud incluye información que no está en un formato claro para los Titulares de los Datos? En caso de que así sea, asegurarse que se expliquen los códigos para que la información sea comprendida;
¿Hay terceros involucrados en el tratamiento de Datos Personales del Titular de los Datos dentro del ámbito de la solicitud?;
¿Podría el manejo de la solicitud implicar que Datos Personales de terceros sean comunicados al Titular de los Datos? En caso de que sí, ¿es posible únicamente extraer Datos Personales del solicitante, con esfuerzos razonables y sin riesgo para los Datos Personales de terceros?

Es importante destacar que la recopilación de dicha información debe limitarse a lo que esté actualmente disponible en Concentrix. No se recopilará información adicional.

Los Miembros de las BCR **deberán abstenerse, lo más posible, de comunicarse con el Titular de los Datos, incluso si el Cliente lo requiere. Cuando se envíe tal solicitud a un Miembro de las BCR, este deberá primero discutir con el Cliente la verdadera oportunidad de que Concentrix establezca contacto directo con el Titular de los Datos. Si el Miembro de las BCR acepta los contactos directos con el Titular de los Datos, dicho Miembro de las BCR deberá informar al Cliente que este último mantiene toda la responsabilidad frente al Titular de los Datos para manejar adecuadamente dicha Solicitud.**

Identificación del tipo de respuesta

El Líder de Privacidad Local deberá asegurarse de que examine la información proporcionada por el Cliente y por el Titular de los Datos dentro de los 8 días hábiles siguientes a la recepción de la Solicitud para determinar si:

Tiene la información apropiada para manejar la Solicitud; y
Considera que la Solicitud es razonable (a diferencia de una Solicitud sin prueba de identidad del Titular de los Datos, una demanda excesiva resultante de Solicitudes repetitivas, Solicitudes de Datos Personales ya eliminados de acuerdo con el período de retención, Solicitudes en nombre de otros, etc.).

A continuación, son posibles tres casos. Estos son los siguientes:

(i) **Caso 1**

Cuando la información dada por el Titular de los Datos **no es suficiente** para manejar la solicitud, el Líder de Privacidad Local, o cualquier otro individuo o entidad, interna o externa designada por el Líder de Privacidad Local con el propósito del manejo de las siguientes responsabilidades, deberá enviar una solicitud al Cliente para información adicional a no más tardar 2 días laborales luego de recibir la solicitud.

Cuando la solicitud sea demasiado compleja y sujeta a conformidad con cualquier requerimiento legal, la línea de tiempo de respuesta podría ser extendida hasta a **20 días laborales**, sujeto a documentación del análisis de complejidad por el Líder de Privacidad Local.

(ii) **Caso 2**

Cuando el Líder de Privacidad Local considere en su análisis inicial, que la solicitud podría **no ser razonable**, no debería inmediatamente concluir el caso. El Líder de Privacidad Local, o cualquier otro individuo o entidad, interna o externa, designada por el Líder de Privacidad Local con el propósito del manejo de las siguientes responsabilidades, deberá responder al Cliente **en los próximos 10 días laborales** luego de recibir la solicitud, requiriendo al Cliente proveer más información del porqué el Titular de los Datos tiene la intención de ejercer esos derechos.

Al recibir la información adicional, si el Líder de Privacidad Local aún considera que la Solicitud presentada por el Titular de los Datos no es razonable, el Líder de Privacidad Local deberá documentar por qué considera que la Solicitud no es razonable y deberá asegurarse, después de la aprobación escrita del DPO, de responder al Cliente o al Titular de los Datos, si así lo instruye expresamente el Cliente, a más tardar **15 días hábiles** después de recibir la información adicional.

La respuesta deberá incluir el motivo por el cual no se toma ninguna acción y la posibilidad para el Titular de los Datos de presentar una queja ante una autoridad de protección de datos y buscar un remedio judicial. La redacción de dicha respuesta deberá ser validada por el DPO y el Cliente.

Cuando el Líder de Privacidad Local considere que, con base en los elementos adicionales, la Solicitud puede ser atendida, deberá asegurarse de que se aborde la solicitud dentro de los **15 días hábiles** mencionados anteriormente y deberá informar al DPO en consecuencia.

(iii) **Caso 3**

Cuando la información proporcionada por el Cliente y/o el Titular de los Datos sea suficiente, el Líder de Privacidad Local deberá asegurarse de que responda a la Solicitud, de acuerdo con las instrucciones del Cliente, dentro de los **15 días hábiles** siguientes a su recepción y deberá informar por escrito al DPO sobre el tiempo y el contenido de la respuesta proporcionada.

3.3.1. Proceso de Escalación

En caso de una queja recibida directamente del Titular de los Datos sobre cómo se ha abordado su Solicitud, ya sea durante o después de haber dado la respuesta, el Líder de Privacidad Local deberá asegurarse de que comparta el asunto con el

Cliente y el DPO, **a más tardar 3 días hábiles** después de recibir la queja del Titular de los Datos.

Para cada uno de los pasos anteriores, y cuando sea necesario para manejar el caso adecuadamente, el Líder de Privacidad Local deberá estar dispuesto a cooperar con el DPO proporcionando a este cualquier información relevante en relación con el asunto e informar al Cliente sobre el manejo del procedimiento.

La orientación del Oficial de Protección de Datos del Grupo será vinculante. Sin embargo, el DPO no deberá contactar directamente con el Titular de los Datos, a menos que el Cliente y el Líder de Privacidad Local lo requieran expresamente.

3.3.2. Rechazo de una Solicitud

Aunque los Miembros de las BCR están comprometidos a manejar las Solicitudes de los Titulares de los Datos de manera eficiente, bajo ciertas circunstancias como se define a continuación, los Miembros de las BCR pueden tener el derecho de no aceptar la Solicitud del Cliente o del Titular de los Datos.

Los Miembros de las BCR pueden oponerse a la Solicitud del Cliente o del Titular de los Datos, cuando aceptar la Solicitud implique que se compartirá la siguiente información:

información cubierta por el privilegio legal;
información que un Miembro de las BCR tiene legalmente prohibido comunicar;
y/o
información que un Miembro de las BCR está procesando durante el curso de una investigación en curso o un procedimiento judicial pendiente.

Cuando haya un conflicto de privacidad, los Datos Personales pueden ser redactados antes de ser compartidos con el Cliente o el Titular de los Datos.

Adicionalmente, en caso de una Solicitud recibida del Cliente en relación con un Titular de los Datos que se opone al procesamiento adicional de sus Datos Personales y/o solicita la eliminación de sus Datos Personales, los Miembros de las BCR pueden rechazar dicha Solicitud cuando las obligaciones legales impidan a los Miembros de las BCR hacerlo o cuando los Miembros de las BCR tengan un interés legítimo preeminente. Esto deberá evaluarse caso por caso y referirse al DPO para una decisión final antes de informar al Cliente o al Titular de los Datos.

3.4. Comunicación con el Titular de los Datos

Si el Cliente requiere que los Miembros de las BCR manejen la Solicitud en su nombre, se aplicarán las siguientes reglas cuando los Miembros de las BCR se comuniquen con el Titular de los Datos.

Bajo ninguna circunstancia y a menos que el Cliente lo indique expresamente, los Miembros de las BCR deberán contactar al Titular de los Datos durante todo el procedimiento. Incluso si lo requiere el Cliente, los Miembros de las BCR deberán abstenerse, en la medida de lo posible, de comunicarse con el Titular de los Datos.

Al comunicarse con el Titular de los Datos, los Miembros de las BCR deberán cooperar con el Titular de los Datos y atender cualquier Solicitud de manera oportuna. Toda comunicación deberá proporcionarse utilizando un lenguaje claro y sencillo, en una forma inteligible, concisa, fácilmente accesible y comprensible.

La información que se debe proporcionar a los Titulares de los Datos deberá ser precisa y limitada a (i) lo que el Titular de los Datos ha solicitado y (ii) la lista de información que puede ser proporcionada por un Responsable de Datos de acuerdo con la Legislación Aplicable de Protección de Datos.

El Líder de Privacidad Local deberá prestar especial atención a los plazos mencionados en este Procedimiento.

Como regla general, los Miembros de las BCR no deberán aplicar tarifas para Solicitudes razonables de los Titulares de los Datos. Sin embargo, bajo ciertas circunstancias, en particular cuando el manejo de la Solicitud implique esfuerzos importantes por parte de los Miembros de las BCR, se podrán aplicar tarifas razonables, sujetas a un máximo nacional de acuerdo con las leyes aplicables, siempre que el Titular de los Datos sea informado sobre dichas tarifas con antelación.

-

Preguntas acerca de este procedimiento o conocimiento de alguna violación o potencial violación al procedimiento debe ser reportado directamente al Oficial de Protección del Grupo.

Apéndice 11A
Alcance del material de las BCR para el Responsable

Lista de Propósitos del Tratamiento y Categorías relacionadas de Datos Personales y Titulares de los Datos

Además de las disposiciones de la sección 2.1 sobre el alcance material de estas BCR-C, la tabla a continuación proporciona más detalles sobre las Transferencias realizadas bajo estas BCR-C. Esta tabla detalla el Propósito del Tratamiento y las categorías relacionadas de Titulares de los datos y Datos Personales cubiertos por la presente BCR-C. La tabla proporcionada en la sección 1 a continuación ofrece detalles sobre las transferencias de datos personales realizadas entre los Miembros de la BCR enumerados en el Apéndice 1 bajo esta BCR-C.

Los países a los que se pueden transferir los Datos Personales dependen de la localización de los Miembros de las BCR involucrados en las actividades de Tratamiento y se proporcionan en el Apéndice 1. Cabe señalar que, en lo que respecta a las BCR-C, las Transferencias de Datos Personales ocurren principalmente entre los Miembros de las BCR de una misma Región (excepto para las entidades Globales, donde puede haber transferencias entre dichas entidades Globales y todos los demás Miembros de las BCR dependiendo de los Propósitos del Tratamiento). Para mayor transparencia, hemos incluido una tabla adicional que presenta las Regiones en la sección 2 del presente Apéndice.

1. Tabla sobre las Transferencias de Datos Personales entre los Miembros de las BCR enumeradas en el Apéndice 1 bajo esta BCR-C

Ámbito de las actividades de tratamiento	Propósito del tratamiento	Categorías de datos personales	Categorías de Titulares de Datos
Actividades de tratamiento de RRHH	**Gestión de reclutamiento**	**1.Datos de identificación** (por ejemplo, nombre, apellido, correo electrónico, número de teléfono, foto (si se proporciona), dirección) **2. Datos económicos y financieros** (por ejemplo, expectativas salariales) **3. Datos profesionales** (por ejemplo, CV, experiencia previa, diplomas, certificados, idiomas extranjeros hablados, evaluación de conocimientos y formaciones, número y copia de su permiso de trabajo (solo si es necesario)) **4. Verificación de antecedentes** (resultados de la verificación de antecedentes (solo los resultados y para candidatos exitosos que sean contratados))	**Candidatos**

Ámbito de las actividades de tratamiento	Propósito del tratamiento	Categorías de datos personales	Categorías de Titulares de Datos
	Gestión de registros de empleados (incluye el proceso de incorporación, mantenimiento del registro de empleados de acuerdo con la legislación aplicable, seguimiento administrativo de la medicina ocupacional, directorio interno)	**1.Datos de identificación** (por ejemplo, nombre, apellido, correo electrónico, número de teléfono, foto del titular de datos, dirección, género, estado civil) **2.Datos profesionales** (por ejemplo, CV, historial educativo e información sobre habilidades del empleado, experiencia previa, diplomas/certificados, idiomas extranjeros hablados, evaluación de conocimientos y formaciones, número y copia de su permiso de trabajo (solo si es necesario), número de identificación interna del empleado, ubicación de la oficina, historial laboral anterior, unidad de negocio/división, jefe directo, tipo de contrato) security number) **3. Datos económicos y financieros** (por ejemplo, ingresos/salario, IBAN/BIC) **4.Datos sensibles** (número de seguridad social)	**Empleados de los Miembros de las BCR**
	Gestión de nómina	**1.Datos de identificación** (por ejemplo, nombre, apellidos, correo electrónico, número de teléfono, dirección) **2. Datos profesionales** (por ejemplo, número de identificación interna del empleado, tipo de contrato, horas de trabajo) **3.Datos económicos y financieros** (por ejemplo, datos de pago (horas trabajadas, ausencias, compensaciones y prestaciones, bonificaciones, datos sobre prestaciones y derechos), salario, IBAN/BIC) **4.Datos sensibles** (número de la Seguridad Social)	**Empleados de los Miembros de las BCR**
	Gestión del programa de referidos	**1.Datos de identificación** (por ejemplo, nombre, apellidos, correo electrónico, número de teléfono, dirección) **2. Datos profesionales** (por ejemplo, CV, experiencia previa, diplomas, certificados, idiomas extranjeros hablados, evaluación de conocimientos y formaciones).	**Empleados de los Miembros de las BCR** **Candidatos**

Ámbito de las actividades de tratamiento	Propósito del tratamiento	Categorías de datos personales	Categorías de Titulares de Datos
	Gestión de gafetes para empleados	**1.Datos de identificación**(por ejemplo, nombre, apellidos, número de teléfono) **2.Datos profesionales** (por ejemplo, función del puesto, número de identificación interna del empleado), número de identificación del empleado, zonas autorizadas y horas de trabajo) **3.Datos económicos y financieros** (por ejemplo, pago vinculado al uso del comedor)	**Empleados de los Miembros de las BCR**
	Gestión de la formación de empleados (incluye formación interna y formación para clientes)	**1. Datos de identificación** (por ejemplo, nombre, apellidos, correo electrónico, número de teléfono, dirección) **2. Datos profesionales** (por ejemplo, título del puesto, número de identificación interna del empleado, información sobre formación (tipo de formación, fecha, asistencia, resultados de pruebas, etc.), ubicación de la oficina, historial laboral anterior, unidad de negocio/división, jefe directo)	**Empleados de los Miembros de las BCR**
	Gestión de la carrera y movilidad de empleados	**1. Datos de identificación** (por ejemplo, nombre, apellidos, correo electrónico, número de teléfono, foto (si se proporciona), dirección) **2. Datos profesionales** (por ejemplo, CV, título del puesto actual, experiencia previa, diplomas, certificados, idiomas extranjeros hablados, evaluación de conocimientos y formaciones, número y copia de su permiso de trabajo (solo si es necesario))	**Empleados de los Miembros de las BCR**

Ámbito de las actividades de tratamiento	Propósito del tratamiento	Categorías de datos personales	Categorías de Titulares de Datos
	Verificación de antecedentes de empleados	**1. Datos de identificación** (por ejemplo, nombre, apellidos, correo electrónico, número de teléfono, foto (si se proporciona), dirección) **2. Datos profesionales** (por ejemplo, CV, título del puesto actual, experiencia previa, diplomas, certificados, idiomas extranjeros hablados, evaluación de conocimientos y formaciones, número y copia de su permiso de trabajo (solo si es necesario)) **3. Información de la verificación de antecedentes** (por ejemplo, resultados de la verificación de antecedentes)	**Empleados de los Miembros de las BCR**
	Gestión de ausencias y tiempo de trabajo de empleados	**1. Datos de identificación** (por ejemplo, nombre, apellidos) **2. Datos profesionales** (por ejemplo, número de identificación interna del empleado, ubicación de la oficina, historial laboral anterior, unidad de negocio/división, jefe directo, tipo de contrato, horas de trabajo, horario laboral, ausencias (permisos por enfermedad, vacaciones, etc.))	**Empleados de los Miembros de las BCR**
	Gestión de elecciones profesionales	**1. Datos de identificación** (por ejemplo, nombre, apellidos, edad) **2. Datos profesionales** (por ejemplo, preparación de la lista electoral (identidad de los votantes, edad, antigüedad, colegio), gestión de las solicitudes (identidad, naturaleza del mandato solicitado, información para verificar el cumplimiento de los requisitos de elegibilidad, si corresponde, afiliación sindical declarada por los candidatos) y publicación de los resultados de las elecciones (identidad de los candidatos, mandatos afectados, número y porcentaje de votos obtenidos, identidad de los empleados elegidos y, si corresponde, afiliación sindical de los empleados elegidos).	**Empleados de los Miembros de las BCR**

Ámbito de las actividades de tratamiento	Propósito del tratamiento	Categorías de datos personales	Categorías de Titulares de Datos
	Gestión de los comités de los órganos de representación de empleados	**1. Datos de identificación** (por ejemplo, nombre, apellidos) **2. Datos profesionales** (por ejemplo, convocatorias, documentos preparatorios, informes, diversas actas de los comités de los órganos de representación)	**Empleados de los Miembros de las BCR**
	Gestión del rendimiento y evaluación de empleados	**1. Datos de identificación** (por ejemplo, nombre, apellidos). **2. Datos profesionales** (por ejemplo, información sobre la evaluación: fechas de las entrevistas de evaluación, identidad del evaluador, competencias profesionales del empleado, objetivos asignados, resultados esperados, resultados obtenidos, evaluación de habilidades profesionales basada en criterios objetivos con un vínculo directo y necesario con el puesto, observaciones y deseos formulados por el empleado, previsiones de desarrollo profesional. Para los agentes, la transcripción de las conversaciones telefónicas con el cliente final puede utilizarse con fines de evaluación de calidad).	**Empleados de los Miembros de las BCR**
	Evaluación de calidad de Game-changers	**1.Datos de identificación** (por ejemplo, nombre, apellidos, correo electrónico) **2. Datos profesionales** (por ejemplo, número de identificación interna del empleado, título del puesto, jefes directos, KPIs, objetivos asignados, resultados esperados, resultados obtenidos, evaluación de habilidades profesionales basada en criterios objetivos con un vínculo directo y necesario con el puesto, observaciones y deseos formulados por el empleado, previsiones de desarrollo profesional. La transcripción de las conversaciones telefónicas con el cliente final puede utilizarse con fines de evaluación de calidad, resultados de la evaluación)	**Agentes / operadores de los Miembros de las BCR**
	Programa de Bienestar de los Empleados	**1. Datos de identificación** (por ejemplo, nombre, apellidos, correo electrónico) **2. Datos profesionales** (por ejemplo, número de identificación interna, puntuación	**Empleados de los Miembros de las BCR (moderadores)**

Ámbito de las actividades de tratamiento	Propósito del tratamiento	Categorías de datos personales	Categorías de Titulares de Datos
		de encuestas, conversaciones de cuidado programadas, puesto de trabajo, jefe directo, turnos, horas de trabajo, resultados de evaluación de calidad, etc.)	
	Gestión del programa de **Impact Sourcing (reclutamiento, informes, etc.)**	**1. Datos de identificación** (por ejemplo, nombre, apellidos, correo electrónico, número de teléfono, foto (si se proporciona), dirección) **2. Datos económicos y financieros** (por ejemplo, expectativas salariales) **3. Datos profesionales** (por ejemplo, CV, experiencia previa, diplomas, certificados, idiomas extranjeros hablados, evaluación de conocimientos y formaciones, número y copia de su permiso de trabajo (solo si es necesario), fuente de reclutamiento)	**Candidatos,** **Empleados de los Miembros de las BCR**
	Gestión de viajes y gastos	**1. Datos de identificación** (por ejemplo, nombre, apellidos, dirección) **2. Datos profesionales** (por ejemplo, título del puesto, número de identificación interna del empleado, reserva de reserva, fechas de viaje, justificación del viaje de negocios, jefe directo) **3. Datos económicos y financieros** (por ejemplo, informe de gastos, facturas, IBAN / BIC)	**Empleados de los Miembros de las BCR**
	Gestión de actividades sociales y culturales	**1. Datos de identificación** (por ejemplo, nombre, apellidos, dirección, estado civil/relación) **2. Datos profesionales** (por ejemplo, título del puesto, número de identificación interna del empleado) **3. Datos económicos y financieros** (por ejemplo, ingresos, prestaciones y beneficios reclamados y proporcionados)	**Empleados de los Miembros de las BCR (y sus familiares declarados)**

Ámbito de las actividades de tratamiento	Propósito del tratamiento	Categorías de datos personales	Categorías de Titulares de Datos
Vida y servicios de la empresa	**Gestión de TI (asignación y gestión de equipos informáticos, servicio de asistencia técnica)**	**1. Datos de identificación** (por ejemplo, nombre, apellidos, dirección de correo electrónico) **2. Datos profesionales** (por ejemplo, número de identificación interna del empleado, título del puesto, ubicación de la oficina, jefe directo, información de la solicitud de TI (número de ticket, tema de la solicitud, seguimiento de la solicitud)) **3. Datos técnicos y de conexión** (por ejemplo, dirección IP, información de la cuenta de usuario, ID del dispositivo, aplicaciones profesionales necesarias y sitios web)	**Empleados de los Miembros de las BCR**
	Seguridad de la información interna (prevención del fraude)	**1. Datos de identificación** (por ejemplo, nombre, apellidos, dirección de correo electrónico) **2. Datos profesionales** (por ejemplo, número de identificación interna del empleado, título del puesto, ubicación de la oficina, jefe directo) **3. Datos técnicos y de conexión** (por ejemplo, dirección IP, información de la cuenta de usuario, ID del dispositivo, alertas, resultados de alertas)	**Empleados de los Miembros de las BCR**
	CCTV en las instalaciones de Concentrix	**1. Datos de identificación** (por ejemplo, grabaciones)	**Empleados de los Miembros de las BCR** **Visitantes en los locales de los miembros de las BCR**
	Gestión de la telefonía en el lugar de trabajo	**1. Datos de identificación:** (por ejemplo, nombre, apellidos, dirección de correo electrónico, número de teléfono) **2. Datos técnicos y de conexión** (por ejemplo, dirección IP, inicios de sesión, datos del ID del dispositivo, tipo de teléfono, información relevante sobre el uso de servicios de telefonía y datos necesarios para fines de facturación, incluyendo operador, naturaleza de la llamada (local, nacional, internacional), duración de la llamada, hora y fecha de	**Empleados de los Miembros de las BCR**

Ámbito de las actividades de tratamiento	Propósito del tratamiento	Categorías de datos personales	Categorías de Titulares de Datos
		inicio y finalización de la llamada y factura)	
	Comunicación interna a los empleados (incluyendo comunicación interna por correo electrónico o a través de redes privadas virtuales (intranet))	**1. Datos de identificación** (por ejemplo, nombre, apellido, dirección de correo electrónico). **2. Datos profesionales** (por ejemplo, gráficos, áreas de discusión, áreas de información, aplicaciones y redes). **3. Datos técnicos y de conexión** (por ejemplo, dirección IP, datos del ID del dispositivo, información de la cuenta de usuario).	**Empleados de los Miembros de las BCR**
	Encuesta y formulario para empleados	**1. Datos de identificación** (por ejemplo, nombre, apellido, dirección de correo electrónico, número de teléfono). **2. Datos técnicos y de conexión** (por ejemplo, número de identificación interno del empleado, título del puesto, rol, ubicación de la oficina, resultados anónimos y agregados).	**Empleados de los Miembros de las BCR**
	Directorio interno y gestión de acceso y cuentas de usuarios de los empleados	**1. Datos de identificación** (por ejemplo, nombre, apellido, dirección de correo electrónico). **2. Datos profesionales (**por ejemplo, gráficos, áreas de discusión, áreas de información, aplicaciones y redes). **3. Datos técnicos y de conexión** (por ejemplo, dirección IP, datos del ID del dispositivo, información de la cuenta de usuario).	**Empleados de los Miembros de las BCR**
	Acceso a Internet y control y prevención de la pérdida de datos	**1. Datos de identificación** (por ejemplo, nombre, apellido, dirección de correo electrónico). **2. Datos profesionales** (por ejemplo, número de identificación interno del empleado, título del puesto, rol, ubicación de la oficina, gerente de línea de reporte, aplicaciones y sitios web autorizados, título del puesto del empleado).	**Empleados de los Miembros de las BCR**

Ámbito de las actividades de tratamiento	Propósito del tratamiento	Categorías de datos personales	Categorías de Titulares de Datos
		3. Datos técnicos y de conexión (por ejemplo, dirección IP, datos del ID del dispositivo, información de la cuenta de usuario).	
Legal / Cumplimiento	**Prevención y detección de fraudes**	**1. Datos de identificación** (por ejemplo, nombre, apellido, correo electrónico, número de teléfono). **2. Datos técnicos y de conexión** (por ejemplo, dirección IP, inicios de sesión, datos del ID del dispositivo, datos de interacción, informes de errores, información de monitoreo incorporada en la aplicación, dispositivo utilizado). **3. Datos de interacción necesarios para investigar un posible fraude** (por ejemplo, identificación a través de los medios utilizados para proporcionar los servicios y contactar a los clientes finales; datos de voz del cliente final y del empleado del proveedor de servicios, transcripción de la interacción; número de teléfono, dirección de correo electrónico, planificación de operaciones, indicadores de desempeño de operaciones e indicadores de desempeño de compañeros).	**Empleados de los Miembros de las BCR** **Miembros de las BCR, clientes**
	Sistema de denuncias	**1. Datos de identificación** (por ejemplo, nombre, apellido, correo electrónico, número de teléfono, detalles de las personas autoras de la alerta, de las personas objeto de la alerta y de las personas involucradas en el procesamiento de la alerta). **2. Datos profesionales** (por ejemplo, tipo de contrato, título del puesto, función/trabajo de la(s) persona(s) que reportan el incidente, de la(s) persona(s) implicadas en el incidente y de la(s) persona(s) involucradas en la investigación). **3. Información de la alerta** (por ejemplo, hechos reportados, evidencia como parte de la investigación, registro de seguimientos de la investigación de la alerta).	**Empleados y administradores de los Miembros de las BCR**

Ámbito de las actividades de tratamiento	Propósito del tratamiento	Categorías de datos personales	Categorías de Titulares de Datos
	Gestión de entidades corporativas y legales *(incluyendo mandatos y poderes, delegación de poderes y firmas, informes corporativos (juntas, comités), asociaciones profesionales, directorio de asesores externos)*	**1. Datos de identificación** (por ejemplo, nombre o razón social, correo electrónico, número de teléfono). **2. Datos profesionales** (por ejemplo, CV, registros educativos e información sobre las habilidades del empleado, experiencia previa, diplomas/certificados, idiomas hablados, evaluación de conocimientos y formaciones, número y copia del permiso de trabajo (solo si es necesario), número de identificación interno del empleado, ubicación de la oficina, delegación de autoridades, proxy). **3. Datos económicos y financieros** (por ejemplo, pagos, ingresos/sueldo, situación financiera, facturas, número de tarjeta de crédito, IBAN/BIC).	**Empleados y administradores de los Miembros de las BCR**
	Procedimientos de litigios y disciplinarios de los empleados	**1. Datos de identificación** (por ejemplo, nombre, apellido, correo electrónico, número de teléfono, grabaciones (si es necesario), dirección). **2. Datos profesionales** (por ejemplo, número de identificación interno del empleado, ubicación de la oficina, gerente de línea de reporte, información relacionada con posibles acciones disciplinarias y procedimientos para empleados, naturaleza del litigio relacionado con negocios, título del puesto/función). **3.Información relacionada con el asunto del litigio** (por ejemplo, tema, riesgos estimados, evidencia, etc.).	**Empleados de los Miembros de las BCR** **Abogados**
	Gestión de litigios	**1. Datos de identificación** (por ejemplo, nombre, apellido, correo electrónico, número de teléfono, grabaciones (si es necesario), dirección). **2. Datos profesionales** (por ejemplo, naturaleza del litigio relacionado con negocios, título del puesto/función). **3.Información relacionada con el asunto del litigio** (por ejemplo, tema, riesgos estimados, evidencia, etc.).	**Empleados de los Miembros de las BCR** **Socios comerciales de los miembros de las BCR** **Abogados**

Ámbito de las actividades de tratamiento	Propósito del tratamiento	Categorías de datos personales	Categorías de Titulares de Datos
	Clients and business partners database (empresa a empresa)	**1. Datos de identificación** (por ejemplo, nombre o razón social, correo electrónico, número de teléfono, dirección de la sede). **2. Datos profesionales** (por ejemplo, título del puesto/rol). **3. Datos económicos y financieros** (por ejemplo, pagos, ingresos/sueldo, situación financiera, facturas, número de tarjeta de crédito, IBAN/BIC).	**Socios comerciales/clientes de los miembros de las BCR**
Operaciones y Marketing	**Gestión de clientes y prospectos**	**1. Datos de identificación** (nombre, apellido, correo electrónico, número de teléfono, dirección profesional). **2. Datos profesionales** (título del puesto, rol, nombre de la empresa, ubicación de la oficina). **3. Datos económicos y financieros** (acuerdo con el cliente, factura, requerimientos de pago, órdenes de compra).	**Clientes/prospectos de los miembros de las BCR (contacto comercial)**
	Campañas de marketing directo de Concentrix	**1. Datos de identificación** (nombre, apellido, correo electrónico, número de teléfono, dirección profesional). **2. Datos profesionales** (título del puesto, rol, nombre de la empresa, ubicación de la oficina, decisión de resultado).	**Clientes/prospectos de los miembros de las BCR (contacto comercial)**
	Procesamiento de Servicios de Pago – WPS	**1. Datos de identificación** (por ejemplo, nombre, apellido, documento de identidad, correo electrónico, número de teléfono, dirección postal, género, referencias internas). **2. Datos profesionales** (por ejemplo, información relacionada con la profesión, información sobre la calificación regulatoria de una persona expuesta políticamente). **3. Datos económicos y financieros** (por ejemplo, pagos, ingresos/sueldo, situación financiera, facturas, IBAN/BIC).	**Clientes/prospectos de los miembros de las BCR**
Relaciones con socios/proveedores	**Gestión de proveedores y gestión de contratos**	**1. Datos de identificación** (por ejemplo, nombre, correo electrónico, número de teléfono, dirección de la sede). **2. Datos profesionales** (por ejemplo, títulos de trabajo, copia de acuerdos con proveedores,	**Empleados de los Miembros de las BCR** **Contacto comercial del proveedor**

Ámbito de las actividades de tratamiento	Propósito del tratamiento	Categorías de datos personales	Categorías de Titulares de Datos
		facturas, requerimientos de pago, órdenes de compra).	
	Gestión de relaciones con corredores de datos	**1. Datos de identificación** (por ejemplo, nombre, correo electrónico, número de teléfono, dirección). **2. Datos profesionales** (por ejemplo, título del puesto/rol, gerente de línea de reporte, opción de inclusión/exclusión, aficiones, relación contractual, factura, requerimientos de pago).	**Empleados de los Miembros de las BCR** **Contacto comercial del corredor de datos** **Cliente/Prospecto de Webhelp (contacto comercial)**

2. Tabla sobre las regiones de los Miembros de las BCR

Concentrix Geo/Regiones	Países incluidos en la geografía/región
Grupo (Global)	**Todos los países*** **Las transferencias pueden ocurrir entre entidades globales (incluidas las entidades de Servicios Compartidos Globales) y todas las demás entidades miembros de las BCR del grupo, independientemente del país de ubicación identificado en el Apéndice 1.*
AMERICAS	**Canada** **Colombia** **El Salvador** **Guatemala** **Honduras** **México** **Nicaragua** **Perú** **EE.UU.**

APAC	**Australia** **China** **Hong Kong** **Japón** **Malasia** **Filipinas** **Singapur** **Tailandia**
CRIT	**Albania** **República Checa** **Italia** **Eslovaquia**
DACH	**Austria** **Bosnia y Herzegovina** **Bulgaria** **Alemania** **Hungría** **Kosovo** **Macedonia del Norte** **Polonia** **Eslovenia** **Suiza**
FRANCIA	**Argelia** **Benín** **Francia** **Grecia** **Costa de Marfil** **Madagascar** **Marruecos** **Portugal** **Rumanía** **Senegal**
MET	**Egipto** **Israel** **Jordania** **Arabia Saudí** **Turquía**
PAÍSES BAJOS	**Países Bajos** **Surinam**

NORDICS	**Dinamarca** **Estonia** **Finlandia** **Letonia** **Lituania** **Noruega** **Suecia**
ESPAÑA	**España**
UK	**India** **Sudáfrica** **Reino Unido**
WPS/WKS	**Bélgica** **Francia** **Alemania** **Italia** **Portugal** **España** **Reino Unido** **Estados Unidos** *Las transferencias solo pueden realizarse entre afiliados de WPS/WKS.*
NETINO	**Francia** **Madagascar**
WEBHELP MEDICA	**France** **Portugal** **Spain** *Las transferencias solo pueden realizarse entre afiliados de Webhelp Medica.*

Apéndice 11B
Alcance del material de las BCR para el Encargado

Lista de Propósitos del Tratamiento y Categorías relacionadas de Datos Personales y Titulares de los Datos

Además de las disposiciones de la sección 2.1 sobre el ámbito material de estas BCR-P, la tabla a continuación proporciona detalles adicionales sobre las transferencias realizadas bajo estas BCR-P. Esta tabla detalla el Propósito del Tratamiento y las categorías relacionadas de Titulares de los Datos y Datos Personales cubiertos por las presentes BCR-P. La tabla a continuación proporciona detalles sobre las Transferencias de Datos Personales realizadas entre las Entidades Miembros de las BCR enumeradas en el Apéndice 1 bajo estas BCR-P.

Los países a los que se pueden transferir los datos personales dependen de la localización de los Miembros de las BCR involucrados en las actividades de procesamiento y se proporcionan en el Apéndice 1.

Ámbito de las actividades de tratamiento		Propósito del tratamiento	Categorías de Datos Personales	Categorías de Titulares de los Datos
Operación	Actividades relacionadas con centros de contacto	**Gestión de Operaciones de Centros de Contacto**	**1. Datos de identificación** (por ejemplo, Nombre, Apellido, Correo electrónico, Número de teléfono, Dirección, Código interno de procesamiento que permite la identificación del Cliente Final) **2. Datos profesionales** (por ejemplo, Título del puesto, rol, número de identificación interno del empleado, gerente de línea de reporte) **3. Datos técnicos y de conexión** (por ejemplo, Dirección IP, Inicios de sesión, Datos de ID del dispositivo) **4. Datos de vida personal** (del Cliente Final) (por ejemplo, Estado civil, número de personas en el hogar, número y edad de los hijos en el hogar, ocupación, hábitos de vida y estilo de vida, campo de actividad) **5. Datos de gestión de contratos** (por ejemplo, Número de transacción, detalles de la compra, suscripción, descripción y condiciones del bien o servicio adquirido, Historial de la interacción entre el Cliente Final y el Responsable del Tratamiento) **6. Datos de programas de fidelización y actividades de salida** (por ejemplo, Datos necesarios para la gestión y ciclo de programas de fidelización, prospección, investigación, encuestas, pruebas y promoción de productos) **7. Datos económicos y financieros** (por ejemplo, Información necesaria para gestionar la solicitud del cliente final, como Información sobre pagos, términos de pago (descuentos, rebajas, etc.), detalles bancarios)	**Empleados de los Miembros de las BCR Responsable del Tratamiento / Cliente Final del Cliente / Prospectos** **Empleados y miembros del personal relacionado del Responsable del Tratamiento/Cliente**

Ámbito de las actividades de tratamiento		Propósito del tratamiento	Categorías de Datos Personales	Categorías de Titulares de los Datos
		Operaciones de exclusión (en el transcurso de actividades de salida)	**1.Datos de identificación** (por ejemplo, Nombre, Apellido, Correo electrónico, Número de teléfono, Dirección, Código interno de procesamiento que permite la identificación del Cliente Final) **2.Datos técnicos y de conexión** (por ejemplo, Dirección IP, Inicios de sesión, Datos de ID del dispositivo) **3.Datos de gestión de contratos** (por ejemplo, Información sobre la decisión del Cliente de darse de baja, incluyendo a través de una lista de "no llamar" de terceros)	**Empleados de los Miembros de las BCR** **Responsable del Tratamiento / Cliente Final del Cliente / Prospectos**
		Control de satisfacción del cliente final	**1. Datos de identificación** (por ejemplo, identificación mediante los medios utilizados para interactuar con el Centro de Contacto (número de teléfono, número de fax, dirección de correo electrónico, código interno de procesamiento que permite la identificación del cliente final)) **2. Datos profesionales** (por ejemplo, título del puesto, rol, gerente de línea, ubicación de la oficina) **3. Datos técnicos y de conexión** (por ejemplo, dirección IP, inicios de sesión, datos de identificación del dispositivo) **4. Datos de gestión de contratos** (por ejemplo, respuestas agregadas proporcionadas, resultados de la evaluación)	**Empleados de los Miembros de las BCR** **Responsable del Tratamiento / Cliente Final del Cliente / Prospectos**
		Prevención y detección de fraude	**1. Datos de identificación** (por ejemplo, nombre, apellido, correo electrónico, número de teléfono, dirección, código interno de procesamiento que permite la identificación del cliente final) **2. Datos profesionales** (por ejemplo, título del puesto, rol, gerente de línea, ubicación de la oficina) **3. Datos técnicos y de conexión** (por ejemplo, dirección IP, inicios de sesión, datos de identificación del dispositivo) **4. Datos de interacción** (por ejemplo, información sobre la solicitud del cliente final, respuesta proporcionada, transcripción de la conversación)	**Empleados de los Miembros de las BCR** **Responsable del Tratamiento / Cliente Final del Cliente / Prospectos**

Ámbito de las actividades de tratamiento		Propósito del tratamiento	Categorías de Datos Personales	Categorías de Titulares de los Datos
				Empleados del responsable/clientes y personal relacionado
		Monitoreo, escucha y grabación de interacciones	**1. Datos de identificación** (por ejemplo, nombre, apellido, correo electrónico, número de teléfono, dirección, código interno de procesamiento que permite la identificación del cliente final) **2. Datos profesionales** (por ejemplo, título del puesto, rol, gerente de línea, ubicación de la oficina, número de identificación interno del empleado) **3. Datos técnicos y de conexión** (por ejemplo, dirección IP, inicios de sesión, datos de identificación del dispositivo) **4. Datos de la vida personal** (del cliente final) (por ejemplo, estado civil, número de personas en el hogar, número y edad de los hijos en el hogar, ocupación, hábitos de vida y estilo de vida, campo de actividad) **5. Datos de gestión de contratos** (por ejemplo, número de transacción, detalles de la compra, suscripción, descripción y condiciones del bien o servicio adquirido, historial de la interacción entre el cliente final y el responsable de los datos) **6. Datos de programas de fidelización y actividades externas** (por ejemplo, datos necesarios para la gestión y ciclo de programas de fidelización, prospección, investigación, encuestas, pruebas de productos y promoción) **7. Datos económicos y financieros** (por ejemplo, información necesaria para gestionar la solicitud del cliente final, como	**Empleados de los Miembros de las BCR Responsable del Tratamiento / Cliente Final del Cliente / Prospectos** **Empleados del responsable/clientes y personal relacionado**

Ámbito de las actividades de tratamiento		Propósito del tratamiento	Categorías de Datos Personales	Categorías de Titulares de los Datos
			información sobre pagos, condiciones de pago (descuentos, rebajas, etc.), detalles bancarios) **8. Datos de interacción** (por ejemplo, información sobre la solicitud del cliente final, respuesta proporcionada, transcripción de la conversación)	
		Inteligencia empresarial, informes y análisis	**1. Datos de identificación** (por ejemplo, nombre, apellido) **2. Datos profesionales** (por ejemplo, título del puesto, rol, gerente de línea, ubicación de la oficina) **3. Datos técnicos y de conexión** (por ejemplo, dirección IP, inicios de sesión, datos de identificación del dispositivo) **4. Datos de gestión de contratos** (por ejemplo, estadísticas agregadas sobre el cumplimiento de los KPI impuestos por el cliente)	**Empleados de los Miembros de las BCR** **Responsable del Tratamiento / Cliente Final del Cliente / Prospectos** **Empleados del responsable/clientes y personal relacionado**

Ámbito de las actividades de tratamiento		Propósito del tratamiento	Categorías de Datos Personales	Categorías de Titulares de los Datos
		Numeración y enrutamiento de interacciones / gestión técnica de interacciones	**1. Datos de identificación** (por ejemplo, nombre, apellido, correo electrónico, número de teléfono, dirección, código interno de procesamiento que permite la identificación del cliente final) **2. Datos profesionales** (por ejemplo, título del puesto, rol, gerente de línea, ubicación de la oficina, número de identificación interno del empleado) **3. Datos técnicos y de conexión** (por ejemplo, dirección IP, inicios de sesión, datos de identificación del dispositivo) **4. Datos de gestión de contratos** (por ejemplo, información sobre la decisión del cliente de darse de baja, incluyendo a través de una lista de "no llamar" de terceros)	**Empleados de los Miembros de las BCR** **Responsable del Tratamiento / Cliente Final del Cliente / Prospectos**
		Modificación de la voz del agente para moldear su expresividad y mejorar la comunicación	**1. Datos de identificación** (por ejemplo, Nombre, Apellido, Correo electrónico, Número de teléfono, Dirección) **2. Datos profesionales** (por ejemplo, título del puesto, rol, gerente de línea de reporte, ubicación de la oficina, número de identificación interna del empleado) **3. Datos técnicos y de conexión** (por ejemplo, Dirección IP, Inicios de sesión, Datos del ID del dispositivo)	**Empleados de los Miembros de las BCR**
	Actividades Netino	**Moderación e interacciones sociales en línea**	**1.Datos de identificación** (por ejemplo, Nombre, Apellido, foto del cliente final (si está publicada en la herramienta), Correo electrónico, Número de teléfono, seudónimo) **2.Datos técnicos y de conexión** (por ejemplo, Dirección IP, Inicios de sesión, Datos del ID del dispositivo) **3.Datos de interacción** (por ejemplo, acceso a datos publicados por el interesado en una plataforma)	**Empleados de los Miembros de las BCR** **Responsable del Tratamiento / Cliente Final del Cliente / Prospectos**

Ámbito de las actividades de tratamiento		Propósito del tratamiento	Categorías de Datos Personales	Categorías de Titulares de los Datos
	Servicios relacionados con WPS/WKS	**Recolección y Análisis de Documentos KYC (en nombre de los clientes que realizan el pedido)**	**1.Datos de identificación** (por ejemplo, Nombre, Apellido) **2.Información KYC** (por ejemplo, decisión de continuar/no continuar, resultados de las investigaciones KYC)	**Responsable del Tratamiento / Cliente Final del Cliente / Prospectos**
		Verificación de antecedentes de solicitantes de clientes / KYE (en nombre de los clientes que realizan el pedido)	**1.Datos de identificación** (por ejemplo, Nombre, Apellido) **2.Información KYC** (por ejemplo, decisión de continuar/no continuar, resultados de las investigaciones KYC)	**Responsable del Tratamiento / Cliente Final del Cliente / Prospectos**

Normas Corporativas Vinculativas na Qualidade de Responsável

Nossas BCRs para o **Responsável** aplicam-se exclusivamente à filial da Concentrix sob a Webhelp SAS, que atua como Entidade Europeia Principal. As filiais às quais as BCRs se aplicam estão listadas no Apêndice 01 das BCR.

concentrix

Conteúdo

1. Introdução

Lembrete: Após a transação entre a Webhelp e a Concentrix em setembro de 2023, o nome comercial do grupo agora é Concentrix. No entanto, é importante observar que o alcance das presentes BCR não foi alterado. As BCR são aplicáveis apenas às Afiliadas da Webhelp SAS que atuam como Entidade Europeia Principal. As afiliadas sujeitas às BCR (Controladora e/ou Processadora) estão listadas no Apêndice 01 e serão denominadas Membros das BCR.

No Grupo Concentrix, acreditamos que a proteção dos Dados Pessoais não é apenas uma questão de segurança ou conformidade com um quadro legal específico, mas um compromisso individual e organizacional. A divulgação e o compartilhamento dos padrões da Concentrix através das Normas Corporativas Vinculantes para Processadores (doravante, as "BCR-P") e das presentes Normas Corporativas Vinculantes para Controladoras (doravante, as "BCR-C") são de suma importância em relação às expectativas legítimas dos Titulares dos Dados sobre como seus Dados Pessoais são Processados.

No curso de suas atividades, os Membros das BCR processam tanto Dados Pessoais internos quanto de Clientes. Nesse sentido, os Membros das BCR protegem os Dados Pessoais que processam em seu nome por meio da implementação de medidas e controles técnicos, físicos e administrativos adequados, descritos nas presentes BCR-C. Esses controles garantirão que toda a organização processe Dados Pessoais de maneira consistente, independentemente da natureza e/ou do local do Processamento.

Essa abordagem é particularmente importante devido à diversidade de atividades que a Concentrix realiza em nome de seus Clientes.

Como consequência do acima exposto e considerando os requisitos introduzidos pelo Regulamento Europeu 2016/679 adotado em 27 de abril de 2016 (doravante, o "**Regulamento da UE**" ou "**GDPR**") e as normas, regulamentos e leis aplicáveis no âmbito da proteção de dados, desde que não contrariem o Regulamento da UE, os Membros das BCR Processarão Dados Pessoais de acordo com os seguintes princípios:

- **Legalidade** – Os Dados Pessoais serão coletados e processados quando o Titular dos Dados tiver dado seu consentimento para o Processamento ou quando o Processamento for legítimo ou necessário de acordo com a Legislação Aplicável sobre Proteção de Dados;
- **Lealdade** – O tratamento de Dados Pessoais deve levar em conta as circunstâncias específicas e o contexto em que esses Dados Pessoais são processados;
- **Transparência** – As informações e a comunicação relacionadas com o Tratamento de Dados Pessoais devem ser facilmente acessíveis, fáceis de entender, claras e em uma linguagem simples e direta;
- **Limitação** da finalidade – Os Dados Pessoais serão coletados para finalidades específicas, explícitas e legítimas e não serão processados posteriormente de uma maneira que seja incompatível com essas finalidades;

- **Minimização de dados** – Os Dados Pessoais coletados serão adequados, relevantes e limitados ao necessário em relação às finalidades para as quais são processados;
- · **Exatidão** – Os Dados Pessoais serão exatos e, quando necessário, serão mantidos atualizados. Devem ser tomadas todas as medidas razoáveis para garantir que Dados Pessoais que sejam imprecisos, considerando as finalidades para as quais são processados, sejam eliminados ou retificados sem demora indevida;
- **Limitação de armazenamento –** Os Dados Pessoais devem ser mantidos de forma que permita a identificação dos Titulares dos Dados por não mais do que o tempo necessário para as finalidades para as quais são processados ou qualquer outra retenção legal;
- **Integridade e confidencialidade** – Os Dados Pessoais serão processados de maneira a garantir a segurança adequada, incluindo a proteção contra o processamento não autorizado ou ilícito e contra a perda, destruição ou dano acidental, utilizando medidas técnicas, físicas e administrativas apropriadas.

Através dessas BCR-C, a Concentrix pretende compartilhar e especificar os detalhes e princípios aplicáveis a todos os Membros das BCR e fornecer certos padrões para todo o grupo que permitam a implementação das BCR-C. Além disso, a Concentrix pode disponibilizar políticas específicas, locais ou setoriais. Em caso de contradição entre essas BCR-C e tais políticas específicas, locais ou setoriais, prevalecerão os termos das BCR-C, a menos que as disposições contraditórias dessas políticas específicas, locais ou setoriais protejam melhor os direitos e a liberdade do Titular dos Dados.

Dado que as BCR-C têm como objetivo garantir uma abordagem adequada e consistente em toda a organização da Concentrix em relação ao Processamento de Dados Pessoais, as exceções que podem resultar das legislações aplicáveis não estão refletidas nessas BCR-C. No entanto, essas BCR-C incluem um mecanismo de notificação na seção 12.3, onde a legislação nacional impede que um Membro das BCR cumpra com as BCR-C e quando os Estados-Membros da UE fornecem regras específicas adicionais ao Regulamento da UE. Consequentemente, a legislação local será considerada uma exceção aplicável a essas BCR-C e será registrada de acordo, após a notificação correspondente. Como especificado na seção 12.3, quando essa legislação nacional impuser um nível mais alto de proteção dos Dados Pessoais, essa legislação nacional prevalecerá sobre as BCR-C.

2. Alcance

2.1 Alcance do material

Esta BCR-C é aplicável sempre que um Membro das BCR processe Dados Pessoais como Controlador de dados e como Processador de dados para Processamento realizado dentro da organização da Concentrix, em nome de um Membro das BCR que atue como Controlador de dados.

Devido à ampla gama de atividades cobertas pela Concentrix, a Concentrix pode precisar processar várias categorias em constante evolução de Dados Pessoais, tais como:

- Informações relacionadas com a vida pessoal (por exemplo, gestão de recrutamento, sistema de gravação de câmeras, gestão de clientes e prospects);
- Informações econômicas e financeiras (por exemplo, gestão de folha de pagamento, gestão de clientes e prospects);
- Informações de identificação (por exemplo, gestão de fornecedores, comunicação não comercial, pesquisas e formulários, gestão de clientes e prospects);
- Informações técnicas (por exemplo, gestão de TI e telefonia, gestão de credenciais, gestão de registros de funcionários);
- Informações transacionais (por exemplo, gestão de entidades corporativas e legais).

O alcance do material é detalhado com mais precisão no Anexo 11-A, que fornece uma tabela detalhada sobre o Propósito do Processamento e as categorias relacionadas de Titulares da informação e Dados Pessoais cobertos por este BCR-C. O Anexo 01 fornece informações sobre os países terceiros e os Membros das BCR para os quais os Dados Pessoais são transferidos.

O BCR-C se aplicará a todos os Titulares da informação cujos Dados Pessoais são transferidos dentro do escopo do BCR-C de um Membro das BCR sob o escopo do GDPR. Portanto, o Membro das BCR reconhece que o escopo do BCR-C pode não se limitar a "cidadãos ou residentes do EEE".

Além disso, este BCR-C se aplica ao Processamento de Dados Pessoais por um Membro das BCR que atue como Controlador de dados ou como Processador de dados em nome de outro Membro das BCR que atue como Controlador de dados, independentemente da categoria e natureza desses Dados Pessoais.

Adicionalmente, cada Membro das BCR é também o Controlador dos Dados Pessoais de seus funcionários como seu empregador. Ao Processar Dados Pessoais de seus funcionários, os Membros das BCR cumprirão com este BCR-C e Processarão Dados Pessoais conforme descrito na Política de Privacidade dos Funcionários.

2.2 Alcance Geográfico

A Concentrix deseja implementar, na medida do possível, uma abordagem coerente dentro da organização onde sejam processados Dados Pessoais. Consequentemente, todos os Membros das BCR, independentemente de sua localização ou jurisdição legal, estão sujeitos a este BCR-C. Portanto, este BCR-C se aplicará, no mínimo, a todos os Dados Pessoais transferidos para Membros das BCR fora do EEE e às transferências posteriores para outros Membros das BCR fora do

EEE. Vale lembrar que as entidades da Concentrix vinculadas por este BCR-C (ou seja, os Membros das BCR) estão listadas no Anexo 01.

Como princípio, nenhuma Transferência de Dados Pessoais será realizada por qualquer entidade da Concentrix a menos que e até que esteja vinculada por este BCR-C a uma entidade da Concentrix não vinculada por este BCR-C. Qualquer Transferência desse tipo não poderá ser realizada a menos que essa afiliada da Concentrix tenha fornecido garantias suficientes para implementar medidas técnicas e organizacionais apropriadas de modo que o Processamento e as obrigações relacionadas a esse Processamento atendam aos requisitos deste BCR-C e assegurem a proteção dos direitos dos Titulares da informação.

O Membro das BCR vinculado pelo BCR-C e as entidades da Concentrix não vinculadas assinarão um acordo por escrito para garantir isso.

3. Natureza Vinculante

3.1 Sobre os funcionários da Concentrix

Cada funcionário de um Membro das BCR, como Titular da informação, se beneficiará das disposições deste BCR-C. Dado que a proteção dos Dados Pessoais é uma questão de compromisso individual e organizacional, cada funcionário também deve cumprir os requisitos especificados neste BCR-C.

Assim, o BCR-C faz parte do conjunto de políticas que os funcionários da Concentrix devem seguir como parte de seu contrato de trabalho. O descumprimento dos princípios e regras deste BCR-C pode levar a ações disciplinares que podem resultar na rescisão do contrato e, em certas circunstâncias, em acusações criminais.

3.2 Sobre os Membros das BCR do grupo Concentrix

Como grupo, a Concentrix deseja garantir que todos os Membros das BCR que pertencem a ele estejam vinculados da mesma ou similar maneira aos princípios e obrigações especificados neste BCR-C e cumpram com os requisitos aqui especificados.

Por essa razão, este BCR-C é vinculante para todos os Membros das BCR por meio da assinatura de um Acordo de Transferência de Dados Intragrupo que inclui este BCR-C como um anexo.

A lista de entidades da Concentrix vinculadas por este BCR-C está estabelecida no Anexo 1 deste BCR-C. A Webhelp SAS, como Entidade Europeia Principal, com a assistência do DPO (sigla em inglês para Data Protection Officer), se compromete a manter esta lista atualizada e disponível, e a comunicá-la às partes relevantes conforme determinado ocasionalmente.

3.3 Direcionado aos Encarregados de dados da Concentrix

Quando um Membro das BCR contratar um Processador de dados (seja um Membro das BCR, uma filial do grupo Concentrix que ainda não esteja vinculada pelo BCR ou um fornecedor externo) para realizar atividades específicas de Processamento, esse Processador de dados deverá fornecer garantias suficientes para implementar medidas técnicas e organizacionais apropriadas de modo que o Processamento atenda aos requisitos deste BCR-C.

Portanto, qualquer atividade de Processamento realizada pelos Processadores de dados de um Membro das BCR deverá ser regida por um contrato escrito ou outro ato legal vinculativo e deverá estabelecer todos os elementos do Artigo 28 do GDPR, lembrados a seguir, e em particular o objeto e a duração do Processamento, a natureza e o propósito do Processamento, o tipo de Dados Dados pessoais e as categorias de Titulares das informações e as obrigações e direitos do Membro das BCR que atua como Responsável pelos dados.

Além disso, este contrato ou outro ato legal vinculativo com um Controlador de Dados deverá estabelecer as seguintes disposições:

10. O Controlador de Dados processará os Dados Pessoais exclusivamente de acordo com as instruções documentadas do Responsável pelos Dados, incluindo no que se refere às Transferências de Dados Pessoais, a menos que a legislação da União ou do Estado-Membro ao qual o Controlador de Dados está sujeito exija o contrário (nesse caso, o Controlador de Dados informará o Responsável pelos Dados sobre tal exigência legal antes de realizar o processamento, a menos que tal lei proíba a divulgação dessas informações por razões importantes de interesse público).
11. O Controlador de Dados manterá os Dados Pessoais confidenciais, garantindo especialmente que as pessoas autorizadas a Processar Dados Pessoais tenham se comprometido a manter a confidencialidade ou estejam sujeitas a uma obrigação estatutária adequada de confidencialidade;
12. O Controlador de Dados tomará as medidas de segurança técnicas, físicas e organizacionais adequadas para garantir um nível apropriado de segurança para proteger os Dados Pessoais.
13. O Controlador de Dados não permitirá que o Subcontrolador processe Dados Pessoais em relação às suas obrigações com um Membro das BCR sem a autorização prévia por escrito do Membro das BCR e garantirá que o Subcontrolador se comprometa a cumprir com as mesmas obrigações estabelecidas no ato vinculativo celebrado entre o Controlador de Dados e o Membro das BCR por meio de um contrato ou outro ato legal conforme a legislação da União ou do Estado-Membro. Quando o Subcontrolador não cumprir com suas obrigações de proteção de dados, o Controlador de Dados inicial continuará sendo totalmente responsável perante o Membro das BCR pelo cumprimento das obrigações daquele outro Controlador de Dados.
14. O Controlador de Dados fornecerá todo o suporte necessário ao Membro das BCR em relação ao manejo das solicitações dos Titulares dos Dados relacionadas aos seus direitos.
15. O Controlador de Dados fornecerá toda a assistência razoável ao Membro das BCR para:

- Assegurar um nível de segurança do Processamento adequado ao risco
- Sem demora indevida, informar o Membro das BCR sobre qualquer violação de segurança real ou suspeita que envolva Dados Pessoais e apoiar o Membro das BCR na notificação à Autoridade de Supervisão relevante e na comunicação aos Titulares dos Dados afetados, conforme o caso.
- Realizar uma avaliação de impacto sobre a proteção de dados (DPIA, na sigla em inglês) e, quando relevante, obter a consulta prévia com a Autoridade de Supervisão quando a DPIA indicar um alto risco na ausência de medidas para mitigar o risco.

16. O Controlador de Dados cumprirá as instruções do Membro das BCR relativas à eliminação ou devolução dos Dados Pessoais ao término do contrato ou de outro ato legalmente vinculativo, e eliminará as cópias existentes, a menos que a legislação da União ou do Estado-Membro exija a retenção dos Dados Pessoais.
17. O Controlador de Dados disponibilizará ao Membro das BCR todas as informações necessárias para demonstrar seu cumprimento e contribuirá com auditorias e inspeções realizadas por um Membro das BCR ou por outra autoridade relevante, ou auditoria ordenada pelo Membro das BCR.
18. O Controlador de Dados informará imediatamente ao Membro das BCR se, em sua opinião, uma instrução infringir este BCR-C ou se a Legislação de Proteção de Dados Aplicável for relevante.

4. Princípios para o processamento de dados pessoais

A Legislação Aplicável de Proteção de Dados define um conjunto de princípios que devem ser observados ao Processar Dados Pessoais. A Concentrix se compromete a cumprir esses princípios, atuando como Responsável pelos Dados ou Controlador de Dados em nome de um Membro das BCR que atue como Responsável pelos Dados.

4.1 Definição de uma base legal para o Processamento (Transparência, equidade e licitude)

Quando se processam Dados Pessoais, é necessário que esse processamento tenha uma base legal adequada, conforme previsto no Artigo 6 do RGPD (Regulamento Geral sobre a Proteção de Dados), sendo essa base legal o fundamento que permite o processamento lícito. Os Membros das BCR reconhecem que uma das seguintes bases legais pode ser aplicável para o processamento de Dados Pessoais:

- Consentimento dos Titulares dos Dados;
- Execução de um contrato no qual o Titular dos Dados seja parte ou para a celebração desse contrato;
- Obrigação legal estabelecida pela legislação da União ou do Estado-Membro ao qual o Responsável pelos Dados está sujeito;
- Interesses vitais do Titular dos Dados ou de outra pessoa;

- Execução de uma tarefa realizada no interesse público ou no exercício da autoridade oficial conferida ao Responsável pelos Dados;
- Interesses legítimos do Responsável pelos Dados ou de um terceiro (desde que tais interesses não prevaleçam sobre os direitos e liberdades do Titular dos Dados).
- Ou qualquer outra base legal

Nesse sentido, os Membros das BCR se comprometem a processar Dados Pessoais de maneira lícita somente quando tiverem uma base legal válida para fazê-lo, de acordo com os requisitos da Legislação Aplicável de Proteção de Dados.

Por exemplo, o processamento dos Dados Pessoais dos empregados da Concentrix é necessário para gerenciar as solicitações de permissões (por exemplo, férias). Assim, a base legal para essa operação de processamento decorre da necessidade de executar o contrato de trabalho que a Concentrix e seus empregados assinaram.

Além disso, e em linha com o Artigo 5 a seguir, os Membros das BCR se comprometem a garantir que:

- As Categorias Especiais de Dados Pessoais sejam processadas apenas de acordo com uma das exceções previstas no Artigo 9(2) do RGPD; e
- O Processamento de Dados Pessoais relacionados com condenações penais e delitos esteja proibido, a menos que se apliquem as mesmas exceções previstas no Artigo 10 do RGPD.

4.2 Definição de um propósito (Limitação de propósito)

A menos que esteja especificamente autorizado pela Legislação de Proteção de Dados Aplicável, os Membros das BCR deverão garantir que tenham definido um propósito lícito, justo, explícito e legítimo antes de qualquer coleta ou processamento de Dados Pessoais.

Os Membros das BCR se comprometem a assegurar que os propósitos que definem não infrinjam a Legislação de Proteção de Dados Aplicável e pareçam ser legítimos, ao mesmo tempo em que garantem que os Dados Pessoais não sejam processados posteriormente de uma maneira incompatível com esses propósitos.

Por exemplo, planejar a força de trabalho necessária para fornecer seus serviços e, consequentemente, gerenciar os horários dos empregados da Concentrix é um dos propósitos definidos para a coleta dos Dados Pessoais dos empregados em relação às suas solicitações de permissões.

4.3 Minimização da coleta de Dados Pessoais (Minimização de dados)

Os Membros das BCR se comprometem a coletar e processar Dados Pessoais que sejam estritamente adequados, relevantes e limitados ao que é necessário em relação aos propósitos para os quais são processados.

Os Dados Pessoais não devem ser coletados de forma ampla com a perspectiva de um propósito futuro não definido.

Por exemplo, os Dados Pessoais coletados para gerenciar as solicitações de permissões estão limitados à natureza da permissão (férias, licença maternidade, etc.) e a outras informações relevantes (a duração da permissão), mas não incluem

Dados Pessoais que não sejam estritamente necessários (como com quem o empregado vai de férias, o destino do empregado ou qualquer dado de saúde relacionado a incapacidades).

4.4 Manutenção de um registro

Seja atuando como Responsável pelos Dados ou Controlador de Dados, os Membros das BCR deverão manter um registro de todas as categorias de atividades de processamento de Dados Pessoais sob sua responsabilidade para demonstrar o cumprimento das BCR-C.

Quando atuar como Responsável pelos Dados, o Registro de Atividades de Processamento deverá incluir pelo menos as seguintes informações, de acordo com o Artigo 30.1 do RGPD:

- O nome e os dados de contato da entidade da Concentrix, o possível corresponsável e o Oficial de Privacidade de Dados;
- Os propósitos do processamento;
- A descrição das categorias de Titulares dos Dados e dos Dados Pessoais;
- As categorias de destinatários dos Dados Pessoais;
- As possíveis transferências de Dados Pessoais para um país terceiro ou para uma organização internacional;
- A duração do armazenamento das Informações;
- Uma descrição geral das medidas de segurança técnicas e organizacionais para garantir um nível de segurança adequado ao risco do processamento.

Por exemplo, a operação de processamento para a gestão de solicitações de permissões de empregados está incluída no Registro de Atividades de Processamento relacionado com a gestão administrativa de empregados, que contém as informações listadas anteriormente.

Quando atuar como Controlador de Dados, o Registro de Atividades de Processamento deverá incluir pelo menos as seguintes informações, de acordo com o Artigo 30.2 do RGPD:

- O nome e os dados de contato do(s) Controlador(es) de Dados e de cada Responsável em nome do qual o Controlador atua e, quando aplicável, do representante do Responsável ou do Controlador, e do DPO (Encarregado de Proteção de Dados); • As categorias de processamento realizadas em nome de cada Responsável;
- Quando aplicável, transferências de Dados Pessoais para um país terceiro e, se for o caso, as salvaguardas ou exceções aplicáveis de acordo com o Artigo 49 do RGPD.

4.5 Precisão dos Dados Pessoais (Precisão dos dados)

Os Membros das BCR deverão implementar medidas e controles adequados para garantir que os Dados Pessoais que coletam e processam permaneçam precisos e, quando necessário, sejam mantidos atualizados. Com esse fim, os Membros das BCR se comprometem a adotar as ações necessárias para tomar todas as medidas razoáveis para assegurar que os Dados Pessoais que forem imprecisos, tendo em vista os propósitos para os quais são processados, sejam eliminados ou retificados.

Por exemplo, os empregados têm o dever de informar ao departamento de recursos humanos sobre qualquer atualização em sua situação pessoal (por exemplo, alteração de endereço). Os Membros das BCR garantirão, então, que os Dados Pessoais sejam atualizados de acordo com o registro dos empregados.

4.6 Definição de um período de retenção de dados (Período de armazenamento limitado)

Os Membros das BCR não manterão os Dados Pessoais por um período mais longo do que o estritamente necessário, considerando o propósito para o qual esses Dados Pessoais são coletados. Nesse sentido, os Membros das BCR se comprometem a determinar um período de retenção de dados antes de implementar cada processamento.

Para garantir o cumprimento desse requisito, os Membros das BCR deverão implementar um procedimento de retenção de dados e especificar as diretrizes a serem aplicadas em relação a uma atividade de processamento específica.

Por exemplo, os Dados Pessoais coletados para gerenciar as solicitações de permissões são mantidos pelo tempo necessário para gerenciar os horários, realizar ações relacionadas à folha de pagamento (por exemplo, licença não remunerada) e cumprir com os regulamentos locais aplicáveis sobre prazos e obrigações contábeis.

4.7 Implementação de medidas de segurança (integridade e confidencialidade)

Os Membros das BCR implementaram medidas e controles técnicos, físicos e administrativos apropriados para garantir que os Dados Pessoais não sejam acessados e/ou processados ilegalmente. Tais medidas técnicas, físicas e administrativas devem assegurar um nível de segurança adequado ao risco, incluindo, mas não se limitando a, a destruição, perda, alteração, divulgação não autorizada de, ou acesso a, Dados Pessoais transmitidos, armazenados ou de outra forma processados por qualquer Membro das BCR e qualquer Controlador de dados.

Além disso, os Membros das BCR garantem que seus subcontratados/Controladores de Dados cumpram com as medidas de segurança técnicas e organizacionais implementadas na Concentrix por meio da assinatura de acordos escritos com eles, que compreendam os requisitos estabelecidos no Artigo 28.3 do RGPD (veja também o Artigo 3.3 das BCR-C anteriores).

Por exemplo, os Membros das BCR elaboraram e implementaram uma Política de Segurança da Informação (Apêndice 10 destas BCR-C). Localmente, os Membros das BCR também podem ter implementado políticas de segurança mais específicas. Ao assinar um acordo com subcontratados/Controladores de Dados, os Membros das BCR reservam-se o direito de avaliar o nível de segurança fornecido pela parte contratada para o processamento dos Dados Pessoais.

4.8 Avaliação de Impacto na Proteção de Dados

A Avaliação de Impacto na Proteção de Dados (DPIA, na sigla em inglês) é um processo baseado em riscos introduzido pelo Regulamento Geral sobre a Proteção de Dados (RGPD) que permite ao Responsável pelos Dados descrever o Processamento de Dados Pessoais, demonstrar sua necessidade e proporcionalidade, e ajudar a gerir os riscos para os direitos e liberdades das pessoas naturais resultantes do Processamento de Dados Pessoais, avaliando-os e determinando as medidas para abordá-los. Os membros das BCR se comprometem a realizar as DPIAs de acordo com o **Anexo 09 do Procedimento para a Avaliação de Impacto na Proteção de Dados.**

Quando um tipo de Processamento, que implica particularmente o uso de novas tecnologias, for provável de resultar em um alto risco para os direitos e liberdades dos Titulares dos Dados, os membros das BCR, levando em consideração a natureza, o alcance, o contexto e os propósitos do processamento e antes de sua realização, realizarão uma DPIA. Esse requisito também se aplicará às operações de Processamento existentes quando se prever uma modificação na operação de processamento e tal modificação possa resultar em um alto risco para os direitos e liberdades dos Titulares dos Dados.

O processamento exigirá uma Avaliação de Impacto na Proteção de Dados se atender a dois ou mais dos seguintes critérios:

- O processamento das informações inclui a avaliação ou pontuação sistemática de aspectos pessoais relacionados com pessoas naturais, incluindo a elaboração de perfis e previsões;
- O processamento das informações é baseado em processamento automatizado que afeta significativamente a pessoa natural;
- O processamento das informações é realizado sobre informações sensíveis ou de natureza altamente pessoal;
- A informação é processada em grande escala;
- O processamento combina ou coincide com duas ou mais operações de processamento de informações;
- O processamento das informações inclui uma monitoração sistemática de uma área de acesso público;
- O processamento é realizado sobre informações de pessoas vulneráveis ou crianças;
- O processamento das informações inclui o uso inovador ou a aplicação de soluções tecnológicas ou organizacionais;
- O processamento das informações é realizado para fins diferentes daqueles para os quais os dados foram coletados;
- O processamento das informações impede que os Titulares dos Dados exerçam seus direitos ou utilizem um serviço ou contrato.

Além disso, os membros das BCR realizarão uma DPIA para as operações de Processamento que exigem uma DPIA de acordo com a decisão da lista de operações de processamento de informações que requerem uma DPIA do Órgão de Vigilância correspondente do EEE.

Quando uma DPIA indicar que o Processamento resultaria em um alto risco na ausência de medidas adotadas pelo Responsável pelos Dados para mitigar o risco e quando uma DPIA revelar altos riscos residuais, o membro das BCR buscará a consulta prévia do Órgão de Vigilância do EEE antes de realizar tal Processamento.

Por exemplo, a gestão de solicitações de licença dos empregados não é considerada um processo que apresente um alto risco para os direitos e liberdades dos Titulares dos Dados. No entanto, sempre que um membro das BCR identifique um processamento que atenda a dois ou mais dos critérios mencionados anteriormente, será realizada uma DPIA sob a supervisão do Encarregado de Proteção de Dados (DPO, na sigla em inglês) de acordo com o procedimento descrito no Anexo 9.

4.9 Subprocessamento e Transferências fora do Grupo Concentrix

Os membros das BCR se comprometem a não transferir nenhum Dado Pessoal a Responsáveis pelos Dados e/ou Controladores de Dados que não sejam membros das BCR, a menos que esses Responsáveis e/ou Controladores de Dados forneçam garantias adequadas e tenham implementado medidas técnicas e organizacionais apropriadas, como as previstas nas BCR-C, de forma que o Processamento esteja em conformidade com os requisitos destas BCR-C.

Nesse sentido, os membros das BCR implementaram medidas técnicas, físicas e administrativas adequadas para garantir e controlar que os Dados Pessoais não sejam acessados e/ou processados ilegalmente.

Qualquer membro das BCR está obrigado a celebrar um contrato escrito ou outro ato jurídico vinculativo com qualquer Responsável pelos Dados ou Controlador de Dados fora do Grupo Concentrix (ou não vinculado pelas BCR-C) se estiverem processando Dados Pessoais. O referido contrato ou outro ato jurídico vinculativo deverá estabelecer os elementos mencionados no Artigo 3.3. Esse contrato pode incluir estas BCR-C.

Assim, se um membro das BCR, atuando como Responsável pelos Dados ou Controlador de Dados em nome de outro membro das BCR, utilizar os serviços de um subcontratado estabelecido fora do EEE e precisar, para o propósito dos serviços prestados, compartilhar os Dados Pessoais de seus empregados (somente na medida necessária para as operações), o membro das BCR avaliará, antes da Transferência, se o subcontratado é capaz de cumprir com os requisitos das BCR-C e garantirá a Transferência por meio do ato jurídico vinculativo adequado.

4.10 Implementação de medidas de notificação em caso de violação de Dados Pessoais

Quando ocorrer uma Violação de Dados Pessoais, os membros das BCR deverão seguir o procedimento aplicável de Violação de Dados adotado pela Concentrix.

Em qualquer caso, os membros das BCR deverão, sem demora indevida e, quando possível, no máximo 72 horas após terem tomado conhecimento da Violação de Dados Pessoais, notificar a (1) Webhelp SAS (como o Membro Responsável pelas BCR) e os outros Líderes Locais de Privacidade relevantes quando o membro das BCR atuar como Responsável pelos Dados, assim como o membro das BCR que atuar como Responsável pelos Dados quando um membro das BCR que atuar

como Controlador de Dados se der conta de uma Violação de Dados Pessoais; e (2) ao Órgão de Vigilância competente do EEE, a menos que a Violação de Dados Pessoais seja improvável de resultar em risco para os direitos e liberdades das pessoas naturais.

A notificação mencionada deverá cobrir, pelo menos, as seguintes informações:

- A natureza da Violação de Dados Pessoais e o alcance da Violação de Dados Pessoais, incluindo, quando possível, as categorias e o número aproximado de Titulares dos Dados afetados e as categorias e o número aproximado de registros de Dados Pessoais afetados;
- Nome e dados de contato do Encarregado de Proteção de Dados do Grupo (DPO, na sigla em inglês) ou outro ponto de contato onde se possa obter mais informações;
- Descrição das consequências que provavelmente resultarão da Violação de Dados Pessoais;
- Descrição das medidas tomadas ou propostas pelo Responsável pelos Dados para abordar a Violação de Dados Pessoais, incluindo, quando apropriado, medidas para mitigar seus possíveis efeitos.;
- Descrição das medidas tomadas ou propostas pelo Responsável pelos Dados para abordar a Violação de Dados Pessoais, incluindo, quando apropriado, medidas para mitigar seus possíveis efeitos adversos.

Qualquer membro das BCR, ao processar Dados Pessoais por conta própria como Responsável pelos Dados, e ao processar Dados Pessoais em nome de outro membro das BCR que atue como Responsável pelos Dados, também poderá precisar comunicar aos Titulares dos Dados sobre a Violação de Dados Pessoais quando tal Violação for provável de resultar em um alto risco para os direitos e liberdades das pessoas naturais, de acordo com o Artigo 34 do RGPD. Nessas circunstâncias, a comunicação deverá ser feita sem demora indevida e cobrirá os elementos mencionados anteriormente que seriam comunicados ao Órgão de Vigilância competente do EEE.

Os membros das BCR deverão documentar qualquer Violação de Dados Pessoais e as informações mencionadas anteriormente. Mediante solicitação, os membros das BCR deverão disponibilizar essa documentação ao Órgão de Vigilância competente do EEE.

Em caso de uma violação de segurança que resulte na destruição, perda, alteração, divulgação não autorizada ou acesso acidental ou ilegal aos Dados Pessoais transmitidos, armazenados ou de outro modo processados, os membros das BCR procederão de acordo com o procedimento de Violação de Dados Pessoais descrito no **Anexo 08 Procedimento para a Notificação de Violação de Dados Pessoais.**

5. Tratamento de Dados Sensíveis

Os Membros das BCR comprometem-se a cumprir com as disposições do Artigo 4 – Princípios para o Tratamento de Dados Pessoais e reconhecem que os Dados Pessoais Sensíveis exigem a implementação de uma proteção específica, uma vez que tais Dados Pessoais podem criar riscos significativos em relação aos direitos e liberdades fundamentais do Titular dos dados.

Os Membros das BCR comprometem-se a processar Dados Pessoais Sensíveis de acordo com a Legislação Aplicável de Proteção de Dados e, quando aplicável, com qualquer outro marco setorial adotado pelo Órgão de Vigilância do EEE.

Tal tratamento deve ser limitado e específico, especialmente em relação aos empregados da Concentrix.
Quando um Membro das BCR tiver a intenção de processar Dados Pessoais Sensíveis em seu próprio nome, garantirá que:

- O tratamento seja necessário e legal; ou
- O tratamento seja realizado com salvaguardas e controles adequados; ou
- Quando necessário, o Titular dos Dados tenha dado seu consentimento explícito para o tratamento desses Dados Pessoais Sensíveis para um ou mais fins específicos. Esse consentimento não será considerado necessário quando (1) o Titular dos Dados não estiver em condições de dar seu consentimento e o tratamento for necessário para proteger os interesses vitais do Titular dos Dados ou de outra pessoa; (2) o Titular dos Dados tenha manifestado claramente que os Dados Pessoais Sensíveis afetados são de domínio público; (3) Quando aplicável, o tratamento esteja explicitamente permitido pela Legislação de Proteção de Dados Aplicável ou qualquer lei nacional (por exemplo, registro/proteção de minorias); ou
- Quando necessário, o tratamento é essencial para o propósito de estabelecer, exercer ou defender reivindicações legais, desde que não haja motivos para supor que o Titular dos Dados tenha um interesse legítimo preponderante em garantir que tais dados não sejam tratados.
- Quando necessário, o Tratamento seja essencial para o estabelecimento, exercício ou defesa de reivindicações legais, desde que não haja motivos para supor que o Titular dos Dados tenha um interesse legítimo predominante em garantir que tais dados não sejam processados.

6. Transferência de Dados Pessoais para países terceiros e restrição da Transferência Posterior para Membros que não sejam das BCR

6.1 Transferências e Transferências Posteriores de Dados Pessoais

No decorrer de suas atividades, os Membros das BCR podem transferir Dados Pessoais para outras entidades do grupo Concentrix (sejam ou não Membros das BCR) ou para terceiros. Essas entidades do Concentrix e/ou terceiros podem estar localizados fora do Espaço Econômico Europeu (doravante, "EEE"). Nesse caso, considera-se que ocorrem Transferências de Dados Pessoais. Quando Dados Pessoais forem transferidos, a Concentrix implementará garantias específicas para assegurar que os Dados Pessoais transferidos tenham um nível adequado de proteção, conforme detalhado a seguir:

- As Transferências de Dados Pessoais de um Membro das BCR, atuando como Controlador de Dados, para outro Membro das BCR localizado fora do EEE e atuando como Controlador de Dados ou como Processador de Dados, estarão respaldadas pelas disposições desta BCR-C; ou
- As Transferências de Dados Pessoais de um Membro das BCR atuando como Controlador de Dados para uma entidade do grupo Concentrix

(que não seja um Membro das BCR) ou para terceiros localizados fora do EEE (mais especificamente, em um país fora do EEE que tenha recebido uma decisão de adequação por parte da Comissão Europeia) e que atuem como Processador de Dados estarão respaldadas por um acordo escrito que inclua as cláusulas contratuais padrão aplicáveis adotadas pelo Órgão de Vigilância Competente do EEE e/ou pela Comissão Europeia, como as Cláusulas Contratuais Tipo da Comissão Europeia sobre Transferências (914/2021), Módulo 2 Controlador para Processador; ou

- As Transferências de Dados Pessoais de um Membro das BCR atuando como Controlador de Dados para uma entidade do Concentrix (que não seja um Membro das BCR) ou para terceiros localizados fora do EEE (mais especificamente, em um país fora do EEE que tenha recebido uma decisão de adequação por parte da Comissão da UE) e que atuem como Controlador de Dados estarão respaldadas por um acordo escrito que inclua as cláusulas contratuais padrão aplicáveis adotadas pelo Órgão de Vigilância Competente do EEE e/ou pela Comissão da UE, como as Cláusulas Contratuais Tipo da Comissão Europeia sobre Transferências (914/2021), Módulo 1 Controlador para Controlador.
- Na ausência de uma decisão de adequação ou salvaguardas apropriadas conforme descrito acima, as Transferências podem ser realizadas excepcionalmente se se aplicar uma exceção de acordo com o Artigo 49 do RGPD e devem, quando relevante, ser ocasionais e não repetitivas.

Em qualquer caso, os Membros das BCR comprometem-se a não transferir Dados Pessoais para terceiros que não sejam parte do grupo Concentrix (ou para uma entidade do Concentrix que não seja um Membro das BCR) sem primeiro garantir que seja assegurado um nível adequado de proteção de acordo com o fornecido pelo RGPD, a fim de assegurar que o nível de proteção dos Titulares dos Dados garantido pelo RGPD não seja comprometido.

Mais especificamente, os Membros das BCR concordam que os Dados Pessoais que foram transferidos sob as BCR-C entre dois Membros das BCR só podem ser transferidos posteriormente fora do EEE para Processadores de Dados e Controladores de Dados que não estejam vinculados pelas BCR-C, desde que sejam cumpridos os requisitos sobre Transferências estabelecidos nos Artigos 44 a 46 do RGPD e refletidos neste documento.

6.2 Obrigação do Importador de Dados em caso de solicitação de acesso por parte do governo

Sem prejuízo da obrigação do Membro das BCR que atue como Importador de Dados de informar ao Exportador de Dados sobre sua impossibilidade de cumprir com os compromissos contidos nas BCR-C (Artigo 12.3 a seguir), o Membro das BCR que atue como Importador de Dados notificará imediatamente o Exportador de Dados e, quando possível, o Titular dos Dados (se necessário com a ajuda do Exportador de Dados) se:

- Receber uma solicitação legalmente vinculativa de uma autoridade pública sob as leis do país de destino, ou de outro terceiro país, para a divulgação de Dados Pessoais transferidos de acordo com as BCR-C. Tal notificação incluirá informações sobre os Dados Pessoais solicitados, a autoridade solicitante, a base legal da solicitação e a resposta fornecida;

- Tomar conhecimento de qualquer acesso direto por parte de autoridades públicas aos Dados Pessoais transferidos de acordo com as BCR-C, conforme as leis do país de destino. Tal notificação incluirá todas as informações disponíveis para o Importador de Dados.

Se lhe for proibido notificar o Exportador de Dados e/ou o Titular dos Dados, o Importador de Dados usará seus melhores esforços para obter uma isenção dessa proibição, a fim de comunicar o maior número possível de informações e o mais rapidamente possível, e documentará seus melhores esforços para poder demonstrá-los a pedido do Exportador de Dados.

O Importador de Dados fornecerá ao Membro das BCR que atue como Exportador de Dados, em intervalos regulares, a maior quantidade possível de informações relevantes sobre as solicitações recebidas (em particular, número de solicitações, tipo de dados solicitados, autoridade ou autoridades solicitantes, se as solicitações foram contestadas e o resultado dessas contestações, etc.). Se o Importador de Dados estiver ou se ver parcial ou completamente proibido de fornecer ao Exportador de Dados as informações mencionadas acima, deverá informar o Exportador de Dados sem demora indevida.

O Importador de Dados conservará as informações mencionadas anteriormente enquanto os Dados Pessoais estiverem sujeitos às salvaguardas proporcionadas pelas BCR-C, e as disponibilizará ao Órgão de Vigilância Competente se solicitado.

O Importador de Dados revisará a legalidade da solicitação de divulgação, em particular se ela está dentro dos poderes concedidos à autoridade pública solicitante, e contestará a solicitação se, após uma avaliação cuidadosa, concluir que existem motivos razoáveis para considerar que a solicitação é ilegal de acordo com as leis do país de destino, as obrigações aplicáveis sob o direito internacional e os princípios de cortesia internacional.

O Importador de Dados, nas mesmas condições, buscará possibilidades de apelação.

Ao contestar uma solicitação, o Importador de Dados buscará medidas provisórias para suspender os efeitos da solicitação até que a autoridade judicial competente tenha decidido sobre o mérito da questão. Não divulgará os Dados Pessoais solicitados até que seja exigido a fazê-lo de acordo com as normas processuais aplicáveis.

O Importador de Dados documentará sua avaliação legal e qualquer contestação à solicitação de divulgação e, na medida em que as leis do país de destino permitirem, disponibilizará a documentação ao Exportador de Dados. Também a disponibilizará ao Órgão de Vigilância Competente se solicitado.

O Importador de Dados fornecerá a quantidade mínima de informação permitida ao responder a uma solicitação de divulgação, com base em uma interpretação razoável da solicitação.

Em qualquer caso, as Transferências de Dados Pessoais por um Membro das BCR para qualquer autoridade pública não podem ser massivas, desproporcionais e indiscriminadas de uma maneira que vá além do necessário em uma sociedade democrática (consulte o Artigo 12.3 das BCR-C a esse respeito).

7. Direitos dos Titulares dos Dados

7.1 Direitos de Beneficiários Terceiros

Sempre que um Membro das BCR processe Dados Pessoais como Controlador de Dados ou como Processador de Dados em seu nome, **os Titulares dos Dados têm o direito de fazer cumprir esta BCR-C como beneficiários terceiros.**

Os Titulares dos Dados deverão, no mínimo, poder fazer cumprir os seguintes elementos:

- Base legal para o tratamento (Artigo 4.1);
- Limitação da finalidade do tratamento (Artigo 4.2);
- Minimização dos Dados (Artigo 4.3);
- Limitação dos períodos de armazenamento (Artigo 4.6);
- Exatidão dos Dados (Artigo 4.5);
- Segurança dos Dados Pessoais, especialmente:
    - Proteção de dados desde a concepção e por padrão e medidas para garantir a segurança dos dados (Artigos 12 e 4.7);
    - Notificação de Violação de Dados Pessoais quando a violação de Dados Pessoais possa resultar em um alto risco para seus direitos e liberdades (Artigo 4.10).
- Regras específicas para o tratamento de categorias especiais de Dados Pessoais e Dados Pessoais relacionados a condenações penais e delitos (Artigo 5);
- Transparência e fácil acesso a esta BCR-C (Artigo 12.1);
- Transferências posteriores (Artigo 4.9);
- Direitos de acesso, retificação, eliminação, restrição, notificação sobre a retificação ou eliminação ou restrição a cada destinatário para o qual os Dados Pessoais tenham sido divulgados, objeção ao tratamento, direito à portabilidade dos dados, direito a não ser objeto de decisões baseadas exclusivamente em tratamento automatizado, incluindo a elaboração de perfis (Artigos 7.4 e 7.5);
- Legislação nacional que impeça o cumprimento das BCR (Artigo 12.3) e em caso de solicitações de acesso governamental (Artigo 6.2));
- Direito de apresentar uma reclamação através do mecanismo de queixas interno das empresas (Artigo 8 das BCR e Apêndice 5 – Artigo 3.1);
- Obrigações de cooperação com o Órgão de Vigilância do EEE (Artigo 12.4);
- Direito de apresentar uma reclamação perante o Órgão de Vigilância competente do EEE (escolha perante o Órgão de Vigilância no Estado Membro de sua residência habitual, local de trabalho ou local da suposta infração) e perante o tribunal competente do Estado Membro da UE (escolha do Titular dos Dados para agir perante os tribunais onde o controlador ou processador tenha um estabelecimento ou onde o Titular dos Dados tenha sua residência habitual) (Artigo 8);
- Dever de informar aos Titulares dos Dados sobre qualquer atualização das BCR-C e da lista de Membros das BCR que estejam vinculados por esta BCR-C (Artigo 13);
- · Direitos dos atuais beneficiários terceiros (Artigo 7);

- · Direito a recursos judiciais e direito a obter reparação e, quando aplicável, compensação em caso de descumprimento de um dos elementos exigíveis das BCR-C (Artigos 7 e 8 das BCR, e Apêndice 5 – Artigo 3.4.2).

Portanto, os Membros das BCR reconhecem que os Titulares dos Dados têm o direito de buscar recursos judiciais e/ou recursos perante uma autoridade de proteção de dados nas condições definidas a seguir, por qualquer descumprimento de um dos elementos exigíveis das BCR-C, conforme listado acima, e a receber compensação por qualquer dano resultante da violação das BCR-C por qualquer Membro das BCR.

Um Membro das BCR aceita que os Titulares dos Dados podem ser representados por um organismo, organização ou associação sem fins lucrativos para apresentar a reclamação em seu nome e exercer os direitos listados acima. Esse organismo, organização ou associação deve estar devidamente constituído de acordo com a legislação de um Estado Membro, ter objetivos estatutários de interesse público e estar ativo no campo da proteção dos direitos e liberdades dos Titulares dos Dados no que diz respeito à proteção de seus Dados Pessoais.

Para maior clareza, especifica-se que os direitos dos beneficiários terceiros descritos acima não se estendem aos elementos das BCR-C relacionados com mecanismos internos implementados dentro das entidades, como detalhes de treinamento, programas de auditoria, redes de conformidade e mecanismos para a atualização das BCR-C.

Observe que, sem prejuízo do presente Artigo 7, a Concentrix incentiva os Titulares dos Dados a utilizar o mecanismo de queixas interno descrito no Artigo 8 das BCR-C, que é fornecido a seguir.

7.2 Direito de apresentar uma reclamação e obter recurso judicial, reparação e compensação quando um Membro das BCR dentro do EEE não cumprir com as BCR-C

Quando um Membro das BCR dentro do EEE não cumprir com um dos elementos exigíveis das BCR-C conforme listado na seção 7.1 acima, a Concentrix reconhece que o Membro das BCR dentro do EEE responsável pelo descumprimento assumirá a responsabilidade e tomará as ações necessárias para remediar suas ações.

A Concentrix também reconhece que o Titular dos Dados terá o direito a:

- Apresentar uma reclamação perante um Órgão de Vigilância do EEE, em particular no Estado Membro de sua residência habitual, local de trabalho ou local da suposta infração; e/ou
- Obter um recurso judicial efetivo quando alegar que está BCR-C foi violada por um Membro das BCR como Controlador de Dados ou por um Membro das BCR como Processador de Dados que processe Dados Pessoais em seu nome. A Concentrix reconhece que tal reclamação pode ser apresentada perante o tribunal competente do Estado Membro onde o Membro das BCR

responsável pelo descumprimento está estabelecido ou perante o tribunal onde o Titular dos Dados tem sua residência habitual.

7.3 Direito de apresentar uma reclamação e obter recurso judicial, reparação e compensação quando um Membro das BCR fora do EEE não cumprir com as BCR-C

Quando um Membro das BCR fora do EEE não cumprir com um dos elementos exigíveis das BCR-C listados acima, a Webhelp SAS como Entidade Europeia Principal (1) aceita ser o "Membro Responsável pelas BCR" e, como tal, assume a responsabilidade por qualquer dano material e imaterial resultante do descumprimento das BCR-C, incluindo o pagamento de compensação quando concedido pelo tribunal competente, e (2) compromete-se a tomar as ações necessárias para remediar as ações de tal outro Membro das BCR fora do EEE.

Nessas circunstâncias, a Webhelp SAS também reconhece que qualquer Titular dos Dados que considere que o Membro das BCR localizado fora do EEE (atuando como Controlador de Dados ou Processador de Dados) violou um dos elementos exigíveis listados na Seção 7.1, terá o direito de:

- Apresentar uma reclamação perante uma autoridade de proteção de dados no local onde resida, trabalhe ou onde o Membro das BCR com responsabilidade delegada esteja estabelecido. E/ou
- Obter um recurso judicial efetivo como se a violação tivesse sido causada pela Webhelp SAS em vez do Membro das BCR localizado fora do EEE, perante os tribunais ou autoridades judiciais onde a Webhelp SAS está baseada, ou onde o Titular dos Dados resida ou trabalhe.

Quando os Titulares dos Dados conseguirem demonstrar que sofreram danos e estabelecer fatos que indiquem que é provável que o dano tenha ocorrido devido à violação das BCR-C, a Webhelp SAS será responsável por demonstrar que o Membro das BCR fora do EEE não foi responsável pela violação das BCR-C que resultou nesses danos, ou que não houve tal violação. Caso a Webhelp SAS consiga demonstrar que o outro Membro das BCR localizado fora do EEE não foi responsável pelo ato, também poderá isentar-se de qualquer responsabilidade.

7.4 Direitos dos Titulares de Dados

Os Titulares de Dados têm o direito de usufruir dos seguintes direitos:

- Acessar os Dados Pessoais que lhe dizem respeito e que são processados por um Membro das BCR;
- Solicitar a retificação ou eliminação de qualquer Dado Pessoal impreciso ou incompleto que lhe diga respeito, e de qualquer Dado Pessoal para o qual o propósito do Tratamento já não seja legal ou apropriado;
- Solicitar que o Tratamento dos seus Dados Pessoais que lhe dizem respeito seja limitado;

- Objeção ao Tratamento dos seus Dados Pessoais por um Membro das BCR quando tal Tratamento for necessário para os fins dos interesses legítimos perseguidos pelo Membro das BCR atuando como Controlador de Dados ou por um terceiro, com fins de interesse legítimo, incluindo a elaboração de perfis a qualquer momento, por motivos relacionados com a sua situação pessoal individual, a menos que os interesses perseguidos pelo Membro das BCR prevaleçam sobre os interesses, direitos e liberdades dos Titulares de Dados;
- Objeção ao Tratamento dos seus Dados Pessoais para fins de marketing, incluindo a elaboração de perfis; e
- Receber os seus Dados Pessoais em um formato estruturado, de uso comum, legível por máquina e interoperável quando o Tratamento for realizado por meios automatizados.

Quando um Membro das BCR agir como Controlador, ele deverá lidar com tal solicitação sem demora indevida e de acordo com o procedimento de manejo de reclamações especificado na Seção 8 abaixo.

O Membro das BCR que agir como Controlador deverá comunicar qualquer retificação ou eliminação de Dados Pessoais ou restrição do Tratamento realizada em resposta a uma solicitação do Titular dos Dados a cada destinatário para o qual os Dados Pessoais tenham sido divulgados, a menos que isso seja impossível ou implique um esforço desproporcional. Além disso, esse Membro das BCR deverá informar ao Titular dos Dados sobre esses destinatários, se o Titular dos Dados o solicitar.

7.5 Exercício dos Direitos dos Titulares de Dados

Os Titulares dos Dados têm o direito de fazer cumprir esta BCR-C como beneficiários terceiros e exercer seus direitos em relação ao Tratamento de seus Dados Pessoais por qualquer Membro das BCR que atue como Controlador de Dados. O Membro das BCR deverá garantir que qualquer solicitação ou reclamação do Titular dos Dados em relação ao exercício de seus direitos ("**Solicitações**") seja atendida de maneira oportuna.

Os Titulares dos Dados podem fazer uma solicitação verbal ou por escrito. Os Membros das BCR fornecerão aos Titulares dos Dados meios acessíveis para exercer seus direitos e, em particular:

1 - Um único e-mail dedicado para ser utilizado independentemente do país em que o Titular dos Dados se encontre:

dpo@concentrix.com

Os e-mails locais podem ser usados para levar em conta as especificidades locais, como o idioma.

Para entrar em contato com o seu contato local de privacidade, por favor, consulte o Apêndice 01 - Lista de entidades Concentrix vinculadas pelas BCR-C e contatos locais de privacidade por e-mail.

2 - Portal único com endereço de e-mail do DPO acessível em www.concentrix.com

3 - Endereço postal único para ser utilizado independentemente do país em que o Titular dos Dados se encontre:

Oficial de Proteção de Dados do Grupo

Departamento Jurídico e de Conformidade

3 rue d'Heliopolis

75017 – PARIS

FRANÇA

O DPO, ou qualquer outra pessoa ou entidade, interna ou externa, designada pelo DPO para a gestão das Solicitações, deverá (i) garantir que obteve as informações mínimas necessárias do Titular dos Dados para atender sua Solicitação e (ii) se considerado necessário, obter a maior quantidade possível de informações para permitir que a Solicitação seja gerida adequadamente.

Se houver dúvidas sobre a identidade da pessoa que faz a solicitação, especialmente ao usar meios de comunicação à distância, um Membro das BCR pode precisar solicitar mais informações sobre o Titular dos Dados. As informações coletadas deverão ser (i) limitadas ao necessário para confirmar a identidade da pessoa que faz a solicitação e (ii) não deverão ser coletadas quando os produtos ou serviços fornecidos por um Membro das BCR ou seus Clientes não forem entregues sob a identidade real do usuário. A proporcionalidade deve sempre ser avaliada pelo Responsável pelo Tratamento.

Em qualquer caso, a resposta a um Titular de Dados deverá ocorrer dentro de um prazo máximo de 1 mês após o recebimento da Solicitação. Considerando a complexidade e o número das solicitações, esse prazo de um mês pode ser estendido, no máximo, por dois meses adicionais, caso em que o reclamante deverá ser informado a respeito (conforme detalhado no Apêndice 5).

Quando o Titular de Dados não estiver satisfeito com a resposta inicial fornecida pelo Membro das BCR, esse Titular de Dados terá o direito, em qualquer caso, de solicitar imediatamente que sua Solicitação seja reexaminada. O Titular de Dados deverá fornecer ao Membro das BCR uma explicação detalhada das disposições insatisfatórias da solução fornecida anteriormente. O Membro das BCR deverá levar no máximo 2 meses a partir do recebimento da Solicitação de reexame para determinar como será tratada e deverá informar ao Titular de Dados por escrito a respeito.

Se uma Solicitação ou reclamação do Titular de Dados for rejeitada pelo Membro das BCR ou se a resposta não satisfizer o Titular de Dados, o Titular de Dados poderá, em qualquer caso, entrar em contato com o DPO e/ou apresentar diretamente uma reclamação a um Órgão de Vigilância competente do EEE e/ou buscar um remédio judicial, conforme detalhado anteriormente nas seções 7.1 e 7.2.

Mais detalhes sobre este Artigo estão disponíveis no seguinte apêndice:

- **Apêndice 5 - Procedimento para solicitações dos Titulares de Dados onde a Concentrix atue como Controlador de Dados**

8. Proceso para el manejo de denuncias de los Titulares de los Datos.

Os Titulares dos Dados têm o direito de apresentar uma denúncia diretamente a um Membro das BCR sobre o Processamento de Dados que eles considerem não estar em conformidade com as BCR-C, perante o Membro das BCR que acreditam estar em desacordo. Quando for provável que a violação seja resultado de um ato de um Membro das BCR localizado fora do Espaço Econômico Europeu (EEE), o Titular dos Dados pode apresentar uma denúncia diretamente à Webhelp SAS como a Entidade Europeia Principal.

Os Titulares dos Dados podem apresentar uma denúncia:

(3) Entrando em contato por e-mail com o Líder Local de Privacidade competente do Membro das BCR, no endereço fornecido no Apêndice 01, e/ou

(4) Entrando em contato com o Oficial de Privacidade de Dados do Grupo pelo e-mail dpo@concentrix.com, ou pelo correio postal no endereço

(5) ¾ rue d'Heliopolis, 75017, Paris, França. Essa denúncia será tratada oportunamente pelo membro competente das BCR, com especial cuidado e atenção, de acordo com os passos e o tempo definidos aqui. Essas cláusulas também são aplicáveis em relação às solicitações dos Titulares de Dados para exercer seus direitos (ver Artigo 7 anterior)

Na prática, as denúncias apresentadas pelos Titulares de Dados serão tratadas de acordo com o procedimento definido no **Apêndice 5 – Procedimento para as solicitações dos Titulares de Dados onde a Concentrix atua como Controlador dos Dados**.

O Membro das BCR que atua como Controlador dos Dados deve informar o Titular dos Dados / denunciante sobre as ações tomadas sem atrasos injustificados e, em qualquer caso, dentro de um mês a partir da data em que a denúncia foi apresentada, de acordo com as cláusulas aqui expostas. A denúncia deve ser tratada por um departamento ou pessoa claramente identificados com um nível adequado de independência no exercício de suas funções. Na prática, o departamento ou pessoa competente deve ser o departamento Jurídico e de Conformidade (particularmente, o Oficial e/ou o Líder Local de Privacidade). Considerando a complexidade e o número de solicitações, esse prazo de um mês pode ser estendido por no máximo dois meses adicionais, caso em que o denunciante deve ser informado adequadamente.

Caso o membro competente das BCR decida rejeitar uma denúncia apresentada pelo Titular dos Dados, esse membro se compromete a informar o Titular dos Dados sobre sua decisão e fornecer informações sobre a razão da rejeição.

Caso um Membro das BCR considere que uma denúncia apresentada pelo Titular dos Dados é justificada, esse Membro das BCR se compromete a implementar as medidas corretivas que julgar adequadas para remediar a situação o mais rápido possível. Além disso, o Membro das BCR também informará o Titular dos Dados interessado assim que as medidas corretivas forem implementadas e a situação tiver sido resolvida.

Em qualquer caso, os Membros das BCR reconhecem que os Titulares dos Dados têm o direito de apresentar uma petição perante uma Autoridade de Vigilância do Espaço Econômico Europeu (EEE) e/ou buscar recursos judiciais. Os Membros das

BCR também reconhecem que esses direitos não dependem de os Titulares dos Dados terem utilizado anteriormente o processo para o manejo de denúncias; no entanto, eles são incentivados a fazê-lo.

9. Governança de proteção de dados

A Concentrix definiu uma organização e governança para a proteção de dados, a qual é detalhada no Apêndice 3. Os Membros das BCR (Regras Corporativas de Privacidade) se comprometem a designar um Oficial de Privacidade de Dados, quando necessário, e em conformidade com o Artigo 37 do RGPD, ou qualquer outra pessoa ou entidade (como o responsável pela privacidade) com a responsabilidade de monitorar o cumprimento das BCR-C e que conta com o mais alto suporte administrativo para o cumprimento dessa tarefa. Esta organização é liderada pelo Oficial de Privacidade do Grupo, que depende de uma rede de pontos de contato de privacidade (especificamente os Líderes Regionais de Privacidade, Líderes Locais de Privacidade, além dos Referentes de Privacidade do Negócio) e que podem ser designados como DPO pelo membro competente das BCR.

O DPO formalmente nomeado com um Órgão de Vigilância deve se reportar diretamente ao nível mais alto da administração. Além disso, o DPO pode informar o nível mais alto de administração se surgirem quaisquer perguntas ou problemas durante o exercício de suas funções.

O DPO não deve ter tarefas que possam gerar conflitos de interesse. O DPO não deve realizar avaliações de impacto de proteção de dados, nem auditorias das BCR se tal situação resultar em um conflito de interesse. No entanto, o DPO pode desempenhar um papel muito útil e importante ao auxiliar os Membros das BCR, e devem ser solicitadas sugestões ao DPO.

Os papéis e responsabilidades da rede, assim como sua governança de trabalho, estão definidos em detalhes no **Apêndice 3 – Organização e Governança da Proteção de Dados.**

Além disso, o DPO pode informar o nível mais alto da administração se surgirem perguntas ou problemas durante o exercício de suas funções.

O DPO e os Líderes Locais e Regionais de Privacidade podem ser contatados por meio das informações de contato descritas no Artigo 7.5 das BCR-C e nos contatos de privacidade locais fornecidos no Apêndice 01 das BCR.

10. Treinamento e conscientização

Proteger os Dados Pessoais não é apenas uma questão de cumprir com as leis de privacidade, mas também faz parte da concretização dos valores fundamentais da Concentrix. Nesse contexto, promover uma cultura de privacidade dentro do grupo é essencial para garantir que todos os funcionários, estagiários e outras pessoas cujas condutas no exercício de suas funções estejam sob o controle direto dos Membros das BCR, sejam responsáveis pela proteção dos Dados Pessoais processados como parte de suas operações.

Portanto, essas BCR-C devem ser implementadas adequadamente em toda a organização. Para tal fim, os Membros das BCR adotaram um programa de

treinamento em privacidade, com o objetivo de assegurar que os funcionários da Concentrix, estagiários e outras pessoas cuja conduta, no exercício de suas funções, esteja sob o controle direto dos Membros das BCR, realmente estejam cientes das obrigações, princípios e procedimentos especificados nessas BCR-C. Além dos princípios e obrigações-chave do RGPD, o programa de treinamento e conscientização deve cobrir, entre outros, procedimentos para lidar com solicitações de acesso à informação pessoal por parte das autoridades públicas.

Esse treinamento é direcionado a: (i) pessoas que tenham acesso permanente ou regular aos Dados Pessoais; (ii) pessoas envolvidas na coleta de Dados Pessoais; e/ou (iii) pessoas envolvidas no desenvolvimento de ferramentas utilizadas para processar Dados Pessoais.

O material para o treinamento deve ser atualizado e revisado regularmente, pelo menos anualmente ou após mudanças significativas na Legislação Aplicável de Proteção de Dados, com o objetivo de assegurar que esteja refletido na versão mais recente das BCR-C.

O programa de treinamento tem como objetivo proporcionar:

- Um nível básico de conhecimento fundamental dos princípios que se aplicam ao processar Dados Pessoais e um bom entendimento dos processos existentes e sua implementação; e
- Treinamento específico adaptado às diferentes funções dentro da organização.

Nesse sentido, lembra-se que os Membros das BCR reconhecem que não é possível realizar nenhuma transferência sob as BCR-C para outro Membro das BCR, a menos que este último esteja efetivamente vinculado pelas BCR-C e possa fornecer um treinamento efetivo sobre as BCR-C para os funcionários do respectivo Membro das BCR.

Os Membros das BCR se comprometem a garantir que todos os funcionários da Concentrix, seus estagiários e outras pessoas cujas condutas, no exercício de seu trabalho, estejam sob controle direto dos Membros das BCR, participem do treinamento assim que este esteja disponível e, posteriormente, completem o curso de atualização anual.

No apêndice a seguir, encontram-se mais detalhes sobre este artigo:

- **Apêndice 04 – Programa de Treinamento e Conscientização.**

11. Privacidade desde a concepção / privacidade por padrão

Com o objetivo de garantir que os princípios definidos nesta BCR-C sejam efetivamente considerados e refletidos nos diferentes Processamentos realizados, a Concentrix levará em conta a proteção de dados e implementará medidas técnicas e organizacionais desde o início de qualquer novo projeto.

Para proporcionar um alto nível de proteção aos Dados Pessoais dentro da organização, os princípios e obrigações definidos a seguir serão integrados ao

design de cada projeto, de acordo com os procedimentos de privacidade desde a concepção adotados pela Concentrix.

12. Transparência e Cooperação

12.1 Comunicação das BCR-C

O Membro das BCR compromete-se a assegurar que todos os Titulares dos Dados recebam informações sobre seus direitos como beneficiários terciários em relação ao processamento de seus Dados Pessoais, bem como sobre os meios para exercer esses direitos. Essas informações estão descritas no Artigo 7 das BCR-C.

A Concentrix comunicará abertamente essas BCR-C aos Titulares dos Dados e as tornará facilmente acessíveis a qualquer pessoa. Tal comunicação deve permitir que qualquer Titular dos Dados obtenha uma cópia dessas BCR-C sem atrasos injustificados e em um formato aberto. Além disso, uma versão pública da versão mais recente das BCR-C deve estar disponível a qualquer momento para os Titulares dos Dados no site da Concentrix www.concentrix.com. Os Titulares dos Dados também podem solicitar uma cópia das BCR-C entrando em contato com o DPO em dpo@concentrix.com.

A versão pública das BCR-C deve conter, pelo menos, as seguintes informações:

- Uma descrição do escopo das BCR-C (Artigo 2 das BCR-C),
- A cláusula relacionada com as responsabilidades do Grupo (Artigo 7 das BCR-C), • As cláusulas relacionadas com os princípios de proteção de dados (Artigo 4, 4.1, 4.2, 4.3, 4.5, 4.6, 4.7, 4.9, 4.10 e 5 das BCR-C),
- A legalidade do processamento (Artigo 4.1 e 5 das BCR-C),
- Notificações de segurança e de violações à informação pessoal (Artigo 4.7 e 4.10 das BCR-C)
- Restrições em transferências subsequentes (Artigo 4.9 e Artigo 6 das BCR-C), e
- As cláusulas relacionadas com os direitos dos Titulares dos Dados (Artigo 7, 8 e 12 das BCR-C)).

Essas informações devem ser atualizadas e apresentadas aos Titulares dos Dados de maneira clara, inteligível e transparente. As informações devem ser fornecidas de forma completa; portanto, um resumo deste documento não será suficiente.

A versão pública também deve incluir todas as políticas e procedimentos requeridos anexos às BCR-C como Apêndices, especialmente para as BCR-C:

- Apêndice 01 - Lista dos Membros das BCR vinculados pelas BCR-C e os contatos de e-mail de privacidade local
- Apêndice 02 - Definições para as BCR e procedimentos
- Apêndice 05 - Procedimento para as solicitações dos Titulares dos Dados onde a Concentrix atua como Controladora dos Dados.
- Apêndice 11-A - Escopo material das BCR-C: Lista de finalidades do processamento e categorias relacionadas com os Dados Pessoais e os Titulares dos Dados.

Os outros Apêndices, ou não são aplicáveis às BCR-C, ou são processos internos irrelevantes para que os Titulares dos Dados compreendam ou exerçam seus direitos.

Esses requisitos serão cumpridos garantindo que a versão pública simplificada das BCR-C, que contém todas as informações listadas anteriormente, esteja disponível no site da Concentrix (www.concentrix.com).

A Concentrix promoverá o aprimoramento da cultura de privacidade e segurança dentro de sua organização ao compartilhar essas BCR-C por meio dos sistemas e meios internos (por exemplo, a Intranet da Concentrix, comunicações internas, etc.).)

12.2 Información a los Titulares de los Datos

Os Membros das BCR, quando atuarem como Controladores de Dados, devem fornecer aos Titulares dos Dados qualquer informação exigida pela Legislação Aplicável sobre Proteção de Dados. Os Membros das BCR fornecerão essas informações sem demora e dentro de um período razoável após obter os Dados Pessoais, mas no máximo no prazo de um mês após receber a primeira comunicação ou divulgação a um destinatário legítimo. Tal informação deve conter, pelo menos, os seguintes elementos:

- A identidade e os detalhes de contato do Controlador de Dados; • Os detalhes de contato do Oficial de Proteção de Dados (DPO) e/ou do Líder de Privacidade;
- A finalidade do Processamento e sua base legal;
- Se a informação não for coletada diretamente do Titular dos Dados, as categorias dos Dados Pessoais Processados;
- O destinatário dos Dados Pessoais;
  Caso existam Transferências de Dados fora do EEE, os países para onde os Dados Pessoais serão transferidos, as medidas implementadas para garantir um nível adequado de proteção e os meios pelos quais se pode obter uma cópia dessas medidas ou onde elas estão disponíveis;
- O período de retenção dos dados;
- Os direitos dos Titulares dos Dados conforme definidos no artigo 7 mencionado anteriormente (por exemplo, a existência do direito por parte do Controlador de Dados de solicitar acesso e retificação ou exclusão dos Dados Pessoais, ou restrição do Processamento em relação ao Titular da Informação, ou opor-se ao processamento, bem como o direito à portabilidade dos dados)
- O direito de apresentar uma denúncia a uma autoridade de controle;
- Quando os Dados Pessoais do Titular da Informação são coletados, se o Titular da Informação (1) está obrigado a fornecer os Dados Pessoais devido a qualquer requisito legal ou contratual, ou (2) precisa fornecer os Dados Pessoais para celebrar um contrato, e as possíveis consequências de não fornecer esses dados.
- Se o processamento estiver baseado no consentimento dos Titulares dos Dados, o direito deles de retirar o consentimento a qualquer momento sem afetar a legalidade do Processamento baseado no consentimento antes de sua retirada.

- Se o processamento estiver baseado no interesse legítimo dos Membros das BCR, as explicações desse interesse legítimo.
- Se for o caso, a existência de tomadas de decisões automatizadas, incluindo a elaboração de perfis; e
- Quando os Dados Pessoais não forem coletados do Titular da Informação, qualquer informação disponível sobre suas fontes (por exemplo, em particular, as categorias de Dados Pessoais, a fonte de onde os Dados Pessoais se originam, a natureza pública dos Dados Pessoais));

Os Membros das BCR se comprometem a fornecer essas informações aos Titulares dos Dados em uma linguagem acessível, fácil de entender, clara, simples e direta.

12.3 Inconsistências com as legislações locais e práticas que afetam o cumprimento das BCR-C

Os Membros das BCR se comprometem a usar as BCR-C como ferramenta para as Transferências apenas se for avaliado que a legislação e as práticas em um país terceiro de destino – que não garante um nível adequado de proteção aplicável ao processamento dos Dados Pessoais pelo Membro das BCR que atua como Importador dos Dados, incluindo qualquer requisito para revelar Dados Pessoais ou medidas que permitam o acesso por parte das autoridades públicas – não impedem que este cumpra suas obrigações sob essas BCR-C.

Esse compromisso baseia-se no entendimento de que as leis e práticas, que respeitam a essência dos direitos e liberdades fundamentais, e não excedem o necessário e proporcional em uma sociedade democrática para proteger um dos propósitos listados abaixo, não estão em contradição com as BCR-C:

(u) segurança nacional; e/ou
(v) defesa; e/or
(w) segurança pública; e/ou
(x) a prevenção, investigação, detecção ou processamento de crimes, ou a execução de sanções criminais, incluindo a proteção e prevenção contra ameaças à segurança pública; e/ou,
(y) outros objetivos importantes de interesse público da União ou de um Estado-Membro, particularmente um interesse econômico ou financeiro da União ou de um Estado-Membro, incluindo assuntos monetários, orçamentários e tributários, saúde pública e segurança social; e/ou
(z) A proteção da independência judicial e dos procedimentos judiciais; e/ou
(aa) A prevenção, investigação, detecção e processamento de violações éticas por profissões regulamentadas; e/ou
(bb) Um monitoramento, inspeção ou função regulatória relacionada, mesmo que ocasionalmente, com o exercício da autoridade oficial nos casos referenciados nos pontos (a) até (e); e/ou
(cc) A proteção dos direitos dos Titulares dos Dados e das liberdades de terceiros; e/ou
(dd) A aplicação de ações civis

Na avaliação das leis e práticas do País Terceiro Não Adequado que possam afetar o cumprimento dos compromissos contidos nas BCR-C, os Membros das BCR devem considerar, particularmente, os seguintes elementos:

- **As circunstâncias específicas das transferências** ou grupo de transferências, e qualquer Transferência subsequente prevista dentro do mesmo país terceiro ou para outro País Terceiro Não Adequado, incluindo:
  - Os propósitos para os quais os Dados Pessoais são transferidos e processados (por exemplo, marketing, recursos humanos, armazenamento, suporte de TI, testes clínicos);
  - Tipos de entidades envolvidas no Processamento (o Importador de Dados e qualquer destinatário de qualquer Transferência subsequente) O setor econômico no qual ocorre a Transferência ou grupo de Transferências;

  - Aqui está a tradução para o português brasileiro:

  - As categorias e o formato dos Dados Pessoais Transferidos;
  - Localização do processamento, incluindo o armazenamento; e
  - Canais de transmissão utilizados.
- **As leis e práticas do país terceiro de destino,** relevantes à luz das circunstâncias da transferência, incluindo aquelas que exigem a divulgação dos dados às autoridades públicas ou autorizam o acesso por parte dessas autoridades, bem como aquelas que permitem o acesso a esses Dados Pessoais durante o trânsito entre o país do Exportador de Dados e o país do Importador de Dados, assim como as limitações e salvaguardas aplicáveis.
- **Quaisquer salvaguardas contratuais, técnicas ou organizacionais relevantes** implementadas para complementar as proteções sob as BCR-C, incluindo as medidas aplicadas durante a transmissão e o Processamento dos Dados Pessoais no país de destino.

Quando forem necessárias salvaguardas adicionais às previstas nas BCR-C, a Webhelp SAS, como Membro Controlador das BCR, o DPO e o **Líder Local de Privacidade** correspondente serão informados e envolvidos na avaliação.

Os Membros das BCR devem documentar adequadamente essa avaliação, assim como as medidas complementares selecionadas e implementadas. Essa documentação estará disponível para a Autoridade de Controle competente e para o DPO quando solicitado.

Adicionalmente, o Membro das BCR que atua como Importador dos Dados deve notificar imediatamente o Exportador dos Dados se, ao utilizar essas BCR-C como uma ferramenta para as Transferências, e durante a duração da adesão às BCR, tiver motivos para acreditar que está ou esteve sujeito a leis ou práticas que poderiam impedir o cumprimento de suas obrigações sob as BCR-C, incluindo mudanças subsequentes nas leis do País Terceiro Não Adequado ou uma medida (como uma solicitação de divulgação). Essa informação também deve ser fornecida ao Membro Controlador das BCR e ao DPO.

Após a verificação dessa notificação, o Membro das BCR que atua como Exportador dos Dados, juntamente com o Membro Controlador das BCR, e com a assistência do DPO, do Líder Local de Privacidade competente e da equipe de Segurança da Informação, deve comprometer-se a identificar imediatamente as medidas complementares (como medidas técnicas ou organizacionais para garantir a

segurança e a confidencialidade) que o Membro das BCR que atua como Exportador dos Dados e/ou Importador dos Dados deve adotar para permitir o cumprimento de suas obrigações sob as BCR-C. O mesmo se aplica se um Membro das BCR que atua como Exportador dos Dados tiver motivos para acreditar que um Membro das BCR, atuando como Importador dos Dados, já não pode cumprir suas obrigações de acordo com essas BCR-C.

Quando o Membro das BCR que atua como Exportador dos Dados (juntamente com o Membro Controlador das BCR e o DPO e/ou o Líder Local de Privacidade competente) avaliar que as BCR-C, mesmo se acompanhadas de medidas complementares, não podem ser cumpridas por uma Transferência ou grupo de Transferências, ou se isso for indicado pela Autoridade de Controle competente, esse membro das BCR se compromete a suspender a Transferência ou grupo de Transferências em risco, assim como todas as transferências para as quais a mesma avaliação e raciocínio levariam a um resultado similar, até que a conformidade seja restaurada ou a Transferência seja encerrada.

Após essa suspensão, o Membro das BCR que atua como Exportador dos Dados deve encerrar a Transferência ou grupo de Transferências se as BCR-C não puderem ser cumpridas e a conformidade com as BCR não for restaurada dentro de um mês a partir da suspensão. Neste caso, os Dados Pessoais que tenham sido transferidos antes da suspensão, e qualquer cópia desses dados, deverão, a critério do Membro das BCR que atua como Exportador dos Dados, ser devolvidos a ele ou devem ser destruídos na totalidade.

A Webhelp SAS, como o Membro Controlador das BCR, e o DPO e/ou o Líder Local de Privacidade competente, informarão todos os demais Membros das BCR sobre a avaliação realizada e seus resultados, de modo que as medidas complementares identificadas sejam aplicadas, caso o mesmo tipo de Transferências seja realizado por qualquer outro membro das BCR ou, quando não for possível implementar medidas complementares eficazes, as transferências em questão sejam suspensas ou encerradas.

O Membro das BCR que atua como Exportador dos Dados deve monitorar – de forma contínua e, quando achar apropriado, em colaboração com os Importadores dos Dados – os desenvolvimentos em Países Terceiros Não Adequados para os quais os Exportadores dos Dados tenham transferido Dados Pessoais, que possam afetar a avaliação inicial do nível de proteção e as decisões tomadas em relação a essas Transferências.

12.4 O Dever de Cooperar

Em qualquer caso, os Membros das BCR concordam em cooperar com os Órgãos de Vigilância do EEE, incluindo aceitar auditorias ou inspeções (presenciais ou remotas) por parte desses Órgãos de Vigilância, para considerar as recomendações e acatar a decisão do Órgão de Vigilância competente do EEE em relação às BCR-C. Os Membros das BCR reconhecem e concordam que os poderes e direitos de auditoria do Órgão de Vigilância competente não podem ser limitados, particularmente no que diz respeito às auditorias práticas realizadas por tal Órgão de Vigilância.

Os Membros das BCR e, quando aplicável, seus respectivos representantes devem disponibilizar ao Órgão de Vigilância do EEE, quando solicitado, qualquer informação sobre as operações de processamento cobertas pelas BCR-C, como os registros das atividades de processamento.

Qualquer conflito relacionado ao exercício da supervisão da conformidade com as BCR-C pelo Órgão de Vigilância competente será resolvido nos tribunais do Estado Membro do referido Órgão de Vigilância, de acordo com as leis processuais desse Estado Membro. Os Membros das BCR concordam em se submeter à jurisdição desses tribunais.

13. Programa de Auditoria que abrange as BCR

Cada Membro das BCR que atue como Controlador deve assegurar e ser capaz de demonstrar a conformidade com as BCR-C. Para isso, e adicionalmente aos requisitos estabelecidos no artigo **4.4 (Manutenção de um Registro)**, 4.8 (Avaliação do Impacto sobre a Proteção de Dados) e os Apêndices 08 – Notificação de Violações aos Dados Pessoais, os Membros das BCR devem cumprir os seguintes requisitos sobre o programa de auditoria de proteção de dados.

O Membro das BCR se compromete a desenvolver e integrar em seu programa de auditoria a revisão de sua conformidade com as BCR-C. O programa de auditoria permitirá definir:

- uma frequência razoável para a realização das auditorias;
- o escopo esperado da auditoria; e
- a equipe responsável pela auditoria.

O processo de auditoria é detalhado no **Apêndice 7 – Procedimentos para as Auditorias de Privacidade dos Dados**. A auditoria abrange todos os aspectos desta BCR-C (por exemplo, aplicações, sistemas de TI, bancos de dados que processam os dados pessoais, ou transferências ulteriores, decisões tomadas em relação aos requisitos obrigatórios sob as leis nacionais que entram em conflito com as BCR-C, a revisão dos termos contratuais utilizados para as transferências fora do Grupo para os responsáveis e os encarregados dos dados, as medidas corretivas, etc.), incluindo os métodos e planos de ação que garantam que as medidas corretivas serão implementadas. No entanto, não é necessário que o programa de auditoria monitore necessariamente todos os aspectos das BCR-C que cada membro está auditando, desde que todos os aspectos das BCR-C sejam monitorados em intervalos regulares apropriados para esse Membro das BCR.

Os membros das BCR se comprometem a realizar as auditorias com frequência (pelo menos anualmente e/ou se houver indicadores de não conformidade) para garantir a verificação do cumprimento das BCR-C ou considerando o nível de risco de uma atividade de Processamento coberta pelas presentes BCR-C para os direitos e liberdades dos Titulares dos Dados.

Além das auditorias regulares, auditorias específicas (auditorias ad hoc) podem ser solicitadas pelo DPO e/ou pelo membro da rede de privacidade competente (por exemplo, o Líder Local de Privacidade), ou qualquer outra função competente no grupo Concentrix, como o departamento de auditoria interna. Essas auditorias podem ser realizadas por auditores internos ou externos acreditados,

recomendados pelo DPO e/ou pelo membro competente da rede de privacidade. O plano de auditoria é iniciado e concluído pelo DPO e/ou pelo membro competente da rede de privacidade, conforme especificado no Apêndice 7. Em qualquer caso, os auditores externos devem ser independentes e estar sujeitos a uma obrigação legal de confidencialidade e/ou a uma obrigação legal de confidencialidade adequada.

El DPO é responsável por determinar o escopo das auditorias a serem realizadas. Para tal fim, ele pode consultar o Comitê de Privacidade e/ou encarregar a equipe de auditorias internas da Concentrix para definir o escopo da referida auditoria. A auditoria pode ser conduzida pelo DPO do Grupo e/ou pelos membros competentes da rede de privacidade (por exemplo, o Líder Local de Privacidade) e/ou pela equipe de auditoria interna do grupo Concentrix, ou qualquer outra função relevante dentro da Concentrix, desde que:

- Se garanta a independência das pessoas responsáveis para desempenhar suas funções nessas auditorias; e
-
- · As pessoas encarregadas de auditar o cumprimento das BCR-C não estejam envolvidas em atividades que possam gerar um conflito de interesses.

Os resultados de cada auditoria devem ser apresentados ao DPO do Grupo e/ou aos membros da rede de privacidade (como os Líderes Locais de Privacidade) e/ou ao Comitê de Privacidade e/ou aos membros da diretoria da Webhelp SAS. O relatório final, a identificação de falhas e as ações corretivas devem ser compartilhados e aplicados pelo Líder Local de Privacidade. Com base na avaliação do Líder Local de Privacidade, o relatório também pode ser compartilhado, quando apropriado, com qualquer Referente de Privacidade do Negócio, gerente de segurança local, proprietários do sistema/processo, a diretoria da empresa matriz do grupo Concentrix ou a diretoria do Membro das BCR competente sujeito à auditoria, ou qualquer outro empregado interno necessário. As ações corretivas serão definidas com uma ordem de prioridade para determinar um cronograma de implementação dessas medidas.

A Concentrix reconhece que os Órgãos de Vigilância competentes do EEE podem solicitar a comunicação dos resultados da auditoria e, portanto, concorda em conceder-lhes acesso a esses resultados assim que solicitado. Os resultados dos relatórios de auditoria e os relatórios de auditorias internas relevantes serão preservados de forma que os Órgãos de Vigilância localizados no EEE possam ter acesso a eles, se exercerem seu direito de auditoria conforme estabelecido a seguir.

Os Membros das BCR se comprometem a assegurar que os Órgãos de Vigilância Competentes possam ter acesso aos resultados da auditoria assim que solicitados, e não devem limitar esses direitos, especialmente por motivos de confidencialidade, como, por exemplo, relacionados à proteção de segredos comerciais.

Reforça-se que os Membros das BCR devem autorizar qualquer Órgão de Vigilância competente do EEE a realizar auditorias de proteção de dados sobre qualquer questão relacionada às BCR-C. Nesse sentido, cada membro das BCR deve permitir que o Órgão de Vigilância do EEE audite o Membro das BCR pertinente para que o

Órgão de Vigilância do EEE possa obter as informações necessárias para demonstrar que o(s) Membro(s) está(ão) em conformidade com essas BCR-C (ver também o Artigo 12.4 mencionado anteriormente)..

14. Mudanças nas BCR-C

O DPO da Concentrix, com o apoio dos Líderes Locais de Privacidade, garantirá que as BCR-C sejam mantidas atualizadas (por exemplo, considerando modificações no ambiente regulatório, recomendações das autoridades de proteção de dados da UE ou alterações no escopo das BCR-C).

Em particular, o DPO deve manter uma lista atualizada com as entidades vinculadas pelas BCR-C. Quando qualquer nova entidade da Concentrix se tornar efetivamente vinculada pelas BCR-C (como especificado no Artigo 3.2), o DPO deve atualizar a lista e informar sem demora injustificada a todos os Membros das BCR e aos Órgãos de Vigilância pertinentes do EEE através do Órgão de Vigilância Competente do EEE. Essas informações atualizadas serão disponibilizadas aos Titulares dos Dados juntamente com as BCR-C pelos mesmos meios.

Webhelp SAS reportará essas mudanças ao Órgão de Vigilância do EEE pelo menos uma vez por ano ou quando o DPO considerar necessário. A notificação dessas mudanças aos Órgãos de Vigilância do EEE será realizada pelo menos uma vez ao ano através do Órgão de Vigilância competente, com uma breve explicação das razões que justificam a atualização. Os Órgãos de Vigilância também devem ser notificados pelo menos uma vez por ano, seguindo o mesmo processo, caso não tenha ocorrido nenhuma mudança.

A notificação ou atualização anual também deve incluir a renovação da confirmação de que a Webhelp SAS, como o Membro Responsável das BCR, tomou as providências apropriadas para garantir o pagamento de compensação por qualquer dano resultante de uma violação das BCR-C por Membros das BCR fora do EEE.

Da mesma forma, quando uma emenda tiver um impacto substancial nas BCR-C ou no nível de proteção dos direitos concedidos por essas BCR-C, a Webhelp SAS, com a ajuda do DPO, compromete-se a informar imediatamente aos Membros das BCR e aos Órgãos de Vigilância do EEE.

15. Incumprimento das BCR-C

Ao se constituírem como Membros das BCR, o Exportador de Dados e o Importador de Dados devem cumprir com os seguintes requisitos:

- Nenhuma Transferência Sem Vinculação Eficaz: Não deve ser feita nenhuma transferência para um Membro das BCR a menos que o Membro esteja vinculado de maneira efetiva pelas BCR-C e possa garantir o cumprimento delas.
- Notificação Imediata de Incapacidade de Cumprimento: O Importador dos Dados deve informar imediatamente ao Exportador dos Dados se for

incapaz de cumprir com as BCR-C, por qualquer razão, incluindo as situações detalhadamente descritas no Artigo 12.3 das BCR-C mencionadas anteriormente.

- Suspensão de Transferência em Caso de Violação: Quando o Importador dos Dados violar as BCR-C ou for incapaz de cumpri-las, o Exportador dos Dados deve suspender a Transferência (ver também o Artigo 12.3 das BCR-C mencionadas anteriormente).
- Retorno ou Exclusão de Dados Pessoais: O Importador dos Dados deve, a critério do Exportador dos Dados, devolver ou excluir imediatamente em sua totalidade os Dados Pessoais que tenham sido transferidos sob as BCR-C, quando:
- O Exportador dos Dados tenha suspenso a transferência, e o cumprimento com estas BCR-C não seja restaurado dentro de um prazo razoável, e em qualquer caso dentro de um prazo de um mês após a suspensão; ou
- O Importador dos Dados esteja violando de forma significativa ou persistente as BCR-C.
- O Importador dos Dados não cumpra uma decisão vinculativa de um tribunal competente ou de um Órgão de Vigilância Competente com relação às suas obrigações sob as BCR-C.

Compromissos Relacionados às Cópias dos Dados: Os mesmos compromissos devem ser aplicados a qualquer cópia dos dados. O Importador dos Dados deve certificar a exclusão dos dados ao Exportador dos Dados.

Manutenção do Cumprimento: Até que os dados sejam excluídos ou devolvidos, o Importador dos Dados deve continuar garantindo o cumprimento das BCR-C.

Restrições Legais Locais: No caso de leis locais que se aplicam ao Importador dos Dados proibirem a devolução ou exclusão dos Dados Pessoais transferidos, o Importador dos Dados deve garantir que continuará assegurando o cumprimento das BCR-C, e processará os dados apenas na medida e pelo tempo que a lei local exigir.

Para os casos em que as leis e/ou práticas locais aplicáveis afetarem o cumprimento das BCR-C, veja o Artigo 12.3 das BCR-C mencionadas anteriormente.

16. Terminação

Um Membro das BCR que atue como importador dos Dados e deixe de estar vinculado pelas BCR-C pode conservar, retornar ou excluir os Dados Pessoais recebidos sob as BCR-C.

Se o Exportador dos Dados concordar que os dados sejam armazenados pelo Importador dos Dados, a proteção deve ser mantida de acordo com o Capítulo V do GDPR e conforme refletido no Artigo 6 das BCR-C.

17. Apêndices

- Apêndice 01 - Lista de Membros das BCR vinculados pelas BCR-C e os e-mails de contato de privacidade local
- Apêndice 02 - Definições para as BCR e procedimentos
- Apêndice 03 - Governança e organização da Privacidade
- Apêndice 04 - Programa de conscientização e treinamento sobre privacidade
- Apêndice 05 - Procedimento para as solicitações dos Titulares de Dados quando os Membros das BCR atuam como Controladores de Dados
- Apêndice 06 - Procedimento para as solicitações dos Titulares de Dados quando os Membros das BCR atuam como Processadores de Dados
- Apêndice 07 - Procedimento de Auditoria
- Apêndice 08 - Procedimento em caso de Violação de Dados Pessoais
- Apêndice 09 - Avaliação de Impacto sobre a Proteção de Dados
- Apêndice 10 - Política de Segurança da Informação
- Apêndice 11-A - Lista BCR-C dos propósitos do Processamento e das categorias relacionadas com os Dados Pessoais e os Titulares dos Dados. (Escopo do Material)
- Apêndice 11-B - Lista BCR-P dos propósitos do Processamento e das categorias relacionadas com os Dados Pessoais e os Titulares dos Dados. (Escopo do Material)

CONTROLE DE DOCUMENTO

Versão	Atualização	Resumo das modificações
0.1	27/02/2022	Aprovação Final
0.2	01/01/2023	Atualização da lista de Membros das BCR
0.3	24/02/2023	Atualização da lista de Membros das BCR
0.4	01/04/2024	Rebranding e formatação Alinhamento com as recomendações EDPB 1/2022, revogação e substituição WP256_Rev01

Frequência de Revisão	Este documento será revisado pelo menos anualmente ou em caso de mudanças
Data de emissão	25/05/2018
Domínio	Privacidade
Classificação	Público
Referência	EN__GPPriv-01- Binding Corporate Rules - Controller

Normas Corporativas Vinculativas na Qualidade de Responsável

Nossas BCRs para o **Operador** aplicam-se exclusivamente à filial da Concentrix sob a Webhelp SAS, que atua como Entidade Europeia Principal.

As filiais às quais as BCRs se aplicam estão listadas no Apêndice 01 das BCRs.

concentrix

Conteúdo

1. Introdução

Lembrete: Após a transação entre Webhelp e Concentrix em setembro de 2023, o nome comercial do grupo agora é Concentrix. No entanto, é importante notar que o escopo das presentes BCR não foi alterado. As BCR aplicam-se apenas às Afiliadas da Webhelp SAS que atuem como Entidade Principal Europeia. As afiliadas sujeitas às BCR (Controlador e/ou Operador) estão listadas no Apêndice 01 e serão denominadas Membros das BCR.

No Grupo Concentrix, acreditamos que a proteção dos Dados Pessoais não é apenas uma questão de segurança ou cumprimento de um determinado marco legal, mas um compromisso individual e organizacional. A divulgação e o compartilhamento dos padrões da Concentrix por meio das Regras Corporativas Vinculantes para Operadores (doravante, as "BCR-P") e das presentes Regras Corporativas Vinculantes para Controladores (doravante, as "BCR-C") são de extrema importância em relação às expectativas legítimas dos Titulares dos Dados sobre como seus Dados Pessoais são Processados.

No curso de suas atividades, os Membros das BCR processam tanto Dados Pessoais internos quanto de Clientes. Nesse sentido, os Membros das BCR protegem os Dados Pessoais que processam em seu nome por meio da implementação de medidas e controles técnicos, físicos e administrativos adequados, incluídos nas presentes BCR-P. Esses controles garantirão que toda a organização processe os Dados Pessoais de maneira consistente, independentemente da natureza e/ou do local do Processamento.

Este enfoque é particularmente importante devido à diversidade de atividades que a Concentrix cobre em nome de seus Clientes.

Como consequência disso e levando em consideração os requisitos introduzidos pelo Regulamento Europeu 2016/679 adotado em 27 de abril de 2016 (doravante, o "Regulamento da UE" ou "GDPR") e as normas, regulamentos e leis aplicáveis no âmbito da proteção de dados, desde que não contrariem o Regulamento da UE, os Membros das BCR Processarão os Dados Pessoais de acordo com os seguintes princípios:

- **Licitude** – Os Dados Pessoais devem ser coletados e processados com o consentimento do Titular dos Dados ou quando o Processamento for legítimo ou necessário de acordo com a Legislação Aplicável em Proteção de Dados**;**
- **Lealdade** – O Processamento de Dados Pessoais deve levar em consideração as circunstâncias específicas e o contexto em que esses Dados Pessoais são processados;
- **Transparência** – As informações e comunicações relacionadas com o Tratamento de Dados Pessoais devem ser facilmente acessíveis, fáceis de entender, claras e em uma linguagem simples e direta;
- **Limitação da finalidade** – Os Dados Pessoais devem ser coletados para fins específicos, explícitos e legítimos e não devem ser processados de uma forma que seja incompatível com esses fins;

- **Minimização de dados** – Os Dados Pessoais coletados devem ser adequados, relevantes e limitados ao necessário em relação aos fins para os quais são processados;
- **Precisão** – Os Dados Pessoais devem ser precisos e, quando necessário, atualizados. Devem ser tomadas todas as medidas razoáveis para garantir que Dados Pessoais imprecisos, tendo em vista os fins para os quais são processados, sejam eliminados ou retificados sem demora indevida;
- **Limitação do armazenamento** – Os Dados Pessoais devem ser mantidos de forma que permita a identificação dos Titulares dos Dados por no mais do que o tempo necessário para os fins para os quais são processados ou qualquer outra retenção legal;
- **Integridade e confidencialidade** – Os Dados Pessoais devem ser processados de maneira a garantir uma segurança adequada, incluindo proteção contra o processamento não autorizado ou ilegal e contra a perda, destruição ou dano acidental, utilizando medidas técnicas, físicas e administrativas apropriadas.

Através destas BCR-P, a Concentrix tem a intenção de compartilhar e especificar os detalhes e princípios aplicáveis a todos os Membros das BCR e fornecer certos padrões para todo o grupo que permitam a implementação das BCR-P. Além disso, a Concentrix poderá disponibilizar políticas específicas, locais ou setoriais. Em caso de contradição entre estas BCR-P e tais políticas específicas, locais ou setoriais, prevalecerão os termos das BCR-P, a menos que as disposições contraditórias dessas políticas específicas, locais ou setoriais protejam melhor os direitos e liberdades do Titular dos Dados.

Dado que as BCR-P visam garantir uma abordagem adequada e consistente em toda a organização da Concentrix em relação ao Processamento de Dados Pessoais, as exceções que podem resultar de legislações aplicáveis não são refletidas nestas BCR-P. No entanto, essas BCR-P incluem um mecanismo de notificação no Artigo 13.3, onde a legislação nacional impede que um Membro das BCR cumpra com as BCR-P e onde os Estados Membros da UE fornecem regras específicas adicionais ao Regulamento da UE. Consequentemente, a legislação local será considerada uma exceção aplicável a estas BCR-P e será registrada em consequência, após a notificação correspondente. Como especificado no Artigo 13.3, quando essa legislação nacional impor um nível de proteção mais alto para os Dados Pessoais, essa legislação nacional prevalecerá sobre as BCR-P.

2. Alcance

2.1 Alcance do Material

Esta BCR-P é aplicável sempre que um Membro das BCR processe Dados Pessoais como Operador de dados.

Devido à ampla gama de atividades que a Concentrix cobre e ao fato de que processa principalmente Dados Pessoais em nome de seus Clientes, a Concentrix pode precisar processar várias categorias em constante evolução de Dados Pessoais, tais como:

- Informações relacionadas com a vida pessoal (por exemplo, monitoramento da satisfação do cliente, gestão de interações sociais online);

- Informações econômicas e financeiras (gestão de relações com clientes, prevenção e detecção de fraudes, faturamento, relatórios e análises)
- Informações de identificação (por exemplo, gestão de chamadas recebidas e efetuadas, gestão de operações de exclusão, discagem e roteamento de interações, escuta e gravação de interações);
- Informações técnicas (por exemplo, discagem e roteamento de interações, análise para operações de entrada e saída, solução de análise de voz); ou

El alcance do material é detalhado com mais precisão no **Anexo 11-B**, que fornece uma tabela detalhada sobre o Propósito do Processamento e as categorias relacionadas de Titulares de Dados e Dados Pessoais cobertos por esta BCR-P.

No entanto, esta BCR-P se aplica ao Processamento de Dados Pessoais pelos Membros das BCR que atuam como Operadores de Tratamento, independentemente da categoria e natureza desses Dados Pessoais.

Os Membros das BCR também são os Controladores dos Dados Pessoais de seus funcionários como empregador. Ao processar Dados Pessoais dos funcionários da Concentrix, os Membros das BCR cumprirão com as BCR-C e processarão os Dados Pessoais conforme descrito na Política de Privacidade dos Funcionários.

2.2 Alcance Geográfico

A Concentrix deseja implementar, na medida do possível, uma abordagem consistente dentro da organização onde se processem Dados Pessoais. Em consequência, todos os Membros das BCR, independentemente de sua localização ou jurisdição legal, estão sujeitos a esta BCR-P. Como princípio, nenhuma transferência de Dados Pessoais será realizada por qualquer Membro das BCR a menos que esteja vinculado por esta BCR-P a uma entidade Concentrix que não esteja vinculada por esta BCR-P. Qualquer transferência desse tipo não pode ser realizada a menos que tal entidade Concentrix tenha fornecido garantias adequadas para implementar medidas técnicas e organizacionais apropriadas de modo que o Processamento e as obrigações associadas a esse Processamento cumpram com os requisitos desta BCR-P e assegurem a proteção dos direitos dos Titulares dos Dados. A entidade Concentrix vinculada pelas BCR-P e a entidade Concentrix não vinculada celebrarão um acordo escrito para garantir isso.

3. Natureza Vinculante

3.1 Sobre os empregados da Concentrix

Dado que a proteção dos Dados Pessoais é uma questão de compromisso individual e organizacional, cada funcionário deve cumprir com os requisitos especificados nesta BCR-P.

Em consequência, as BCR-P fazem parte do conjunto de políticas com as quais os funcionários da Concentrix são obrigados a cumprir como parte de seu contrato de trabalho. O descumprimento dos princípios e normas desta BCR-P pode levar a

medidas disciplinares que podem resultar na rescisão do contrato de trabalho e, em certos casos, em acusações criminais.

3.2 Sobre os Membros das BCR do grupo Concentrix

Como grupo, a Concentrix deseja garantir que todos os Membros das BCR pertencentes a ele estejam obrigados da mesma maneira ou de maneira similar aos princípios e obrigações especificados nesta BCR-P e cumpram com os requisitos estabelecidos na mesma.

Por essa razão, esta BCR-P é vinculante para todos os Membros das BCR por meio da assinatura de um Acordo de Transferência de Dados Intragrupo que inclui esta BCR-P como um apêndice.

A lista de entidades da Concentrix vinculadas por esta BCR-P está detalhada no Apêndice 1 desta BCR-P. A Webhelp SAS, como Entidade Europeia Principal, com a assistência do DPO, se compromete a manter essa lista atualizada e disponível, e a comunicá-la mediante solicitação das partes relevantes, conforme determinado ocasionalmente.

3.3 Dirigido aos Operadores de Dados da Concentrix

Quando atuando em nome de seu Cliente como Operador de Tratamento, os Membros das BCR se comprometem a cumprir com esta BCR-P e a implementar os requisitos da mesma em relação aos seus Clientes e aos Titulares dos Dados dos Clientes. Quando os Membros das BCR processarem os Dados Pessoais dos Titulares de Dados de seus Clientes, os Membros das BCR, assim como cada funcionário dos Membros das BCR envolvido no Processamento, se comprometem a garantir, de acordo com as instruções dos Clientes, a proteção dos direitos desses Titulares de Dados e a fornecer um nível adequado de proteção aos Dados Pessoais que processam, sujeito ao disposto na Seção 7 – Direitos dos Titulares dos Dados.

Qualquer atividade de Processamento realizada por um Membro das BCR em nome de um Cliente deve estar regida por um contrato escrito ou outro ato jurídico vinculativo, e deve estabelecer (todos os elementos do artigo 28 do GDPR e, em particular, o objeto e a duração do Processamento, a natureza e o propósito do Processamento, o tipo de Dados Pessoais e as categorias de Titulares dos Dados, assim como as obrigações e direitos do Controlador de Dados). Além disso, este contrato ou outro ato jurídico vinculativo com um Operador de Tratamento deve estabelecer as seguintes disposições:

1. A Concentrix deverá manter os Dados Pessoais confidenciais, especialmente garantindo que as pessoas autorizadas a Processar Dados Pessoais tenham se comprometido com a confidencialidade ou estejam sujeitas a uma obrigação legal de confidencialidade.
2. A Concentrix deverá tomar medidas de segurança técnicas, físicas e organizacionais apropriadas para garantir um nível adequado de segurança para proteger os Dados Pessoais.
3. A Concentrix não permitirá que o Suboperador processe Dados Pessoais em relação à sua obrigação com o Cliente sem a autorização prévia por escrito deste último, e garantirá que o Suboperador se comprometa a cumprir com as mesmas obrigações estabelecidas no ato vinculativo

celebrado entre a Concentrix e o Cliente através de um contrato ou outro ato legal conforme a legislação da União ou dos Estados Membros. Quando o Suboperador não cumprir com suas obrigações de proteção de dados, o Operador de Dados inicial continuará sendo totalmente responsável perante o Membro das BCR pelo cumprimento das obrigações desse outro Operador de Dados.

4. A Concentrix deverá disponibilizar ao Cliente todas as informações necessárias para demonstrar seu cumprimento e contribuir para auditorias e inspeções realizadas pelo Cliente ou por outra autoridade relevante.
5. A Concentrix deverá informar imediatamente ao Cliente sobre qualquer violação de segurança real ou suspeita que envolva Dados Pessoais e apoiar o Cliente na notificação ao Órgão de Supervisão relevante e na comunicação aos Titulares dos Dados afetados, conforme o caso.
6. A Concentrix deverá fornecer toda a assistência razoável ao Cliente para realizar uma avaliação de impacto sobre a proteção de dados.
7. A Concentrix deverá fornecer todo o apoio necessário ao Cliente em relação ao tratamento de solicitações dos Titulares dos Dados relacionadas com seus direitos.
8. A Concentrix deverá cumprir com as instruções do Cliente em relação à eliminação ou devolução dos Dados Pessoais ao final do contrato ou outro ato legal vinculativo.
9. A Concentrix deverá informar imediatamente ao Cliente se, em sua opinião, uma instrução viola esta BCR-P ou a Legislação Aplicável em Proteção de Dados.

Esse contrato incluirá esta BCR-P para divulgar e fazer cumprir as Normas Corporativas Vinculantes perante ambas as partes; os Clientes têm o direito de fazer cumprir qualquer disposição desta BCR-P contra um Membro das BCR ou qualquer Membro das BCR com responsabilidade delegada.

4. Princípios para o Processamento de Dados Pessoais

Quando atuarem em nome de seus Clientes como Operador de Dados, os Membros das BCR deverão cumprir com os princípios definidos a seguir. Em qualquer caso, o Cliente será responsável por todo o Processamento de Dados Pessoais, independentemente da origem dos Dados Pessoais, realizado de acordo com a Legislação Aplicável em Proteção de Dados e o Acordo de Serviço entre a Concentrix e o Cliente.

4.1 Transparência, equidade e legalidade

Quando atuar como Encarregado de Dados, os Membros das BCR se comprometem a (1) fornecer garantias suficientes e implementar medidas técnicas e organizacionais apropriadas de maneira que o Processamento esteja em conformidade com os requisitos desta BCR-P, e (2) cooperar com o Controlador de Dados, dentro de um prazo razoável e na medida razoavelmente possível, e ajudar o Cliente a cumprir a Legislação Aplicável em Proteção de Dados. Como Controlador de Dados, o Cliente dos Membros das BCR continua sendo responsável por garantir que o Processamento que solicita à Concentrix esteja efetivamente em conformidade com a Legislação Aplicável em Proteção de Dados.

Considerando a natureza do processamento e as informações disponíveis, os Membros das BCR, por meio da conclusão do Apêndice de Normas de Processamento de Dados, deverão auxiliar o Cliente quando este considerar que é necessário realizar uma avaliação de impacto sobre a proteção de dados, com base na natureza, alcance, contexto e objetivos do processamento. Na medida em que o Cliente precisar de assistência adicional para realizar uma avaliação de impacto sobre a proteção de dados, para responder a investigações e consultas das autoridades de proteção de dados ou para solicitar uma consulta prévia ao Órgão de Vigilância, os Membros das BCR, considerando a natureza do Processamento e as informações disponíveis para eles, fornecerão assistência ao Cliente por meio do Programa de Auditoria do Controlador de Dados.

Além disso, os Membros das BCR devem garantir que os Dados Pessoais do Cliente armazenados nos sistemas de produção sejam processados pela Concentrix de acordo com o artigo 28.3 (g) do Regulamento da UE, após a rescisão do Acordo de Serviços. A menos que alguma Legislação Aplicável em Proteção de Dados ou qualquer outro Acordo de Serviços exija o armazenamento dos Dados Pessoais e sujeito a solicitação escrita do Controlador de Dados, os Dados Pessoais armazenados nos sistemas de produção devem, a critério do Controlador, ser eliminados ou devolvidos após a rescisão do Acordo de Serviços. Os Membros das BCR devem, dentro do prazo acordado com o Controlador, garantir a confidencialidade dos Dados Pessoais transferidos pelo Cliente e que os Membros das BCR não processarão ativamente os Dados Pessoais transferidos. O Controlador de Dados reconhece que esta eliminação ou restituição de Dados Pessoais (i) será estritamente limitada aos Dados Pessoais fornecidos pelo Controlador e armazenados pela Concentrix, atuando como encarregado, no momento da solicitação e (ii) levará em consideração os requisitos de armazenamento de cópias de segurança e as políticas e padrões de segurança.

Além disso, quando um Membro das BCR tiver razões para acreditar que a legislação aplicável impede esse Membro de cumprir com suas obrigações sob esta BCR-P ou tem um efeito substancial nas garantias fornecidas pelas BCR-P, esse Membro informará imediatamente o DPO, a Webhelp SAS e o outro Líder de Privacidade Local relevante, bem como aos Clientes, conforme estabelecido no Artigo [Erro! Fonte de referência não encontrada.] (exceto quando proibido pela legislação local aplicável ou por uma autoridade de cumprimento da lei, como uma proibição sob a lei penal para preservar a confidencialidade de uma investigação de aplicação da lei). Nesse caso, o Cliente tem o direito de suspender a transferência ou as atividades de Processamento em curso e/ou rescindir o contrato.

4.2 Limitação de propósito

A Concentrix se compromete a cumprir com o princípio geral de limitação da finalidade, segundo o qual processará os Dados Pessoais somente em nome de seu Cliente e em estrita conformidade com suas instruções documentadas, quando atuar como Encarregado de Dados. Os Membros das BCR devem informar imediatamente ao Cliente se, em sua opinião, uma instrução viola a Legislação Aplicável em Proteção de Dados.

Mais concretamente, os Membros das BCR se comprometem a processar os Dados Pessoais em nome de seu Cliente:

- para os únicos fins expressos por esse Cliente;
- sob as condições acordadas entre a Concentrix e seu Cliente em virtude do Acordo de Serviços; e
- pelo tempo não superior ao que esteja expressamente previsto pelo Cliente do Membro das BCR.

Se um Membro das BCR não puder garantir tal conformidade, ele se compromete a informar imediatamente seu Cliente, o DPO e o Líder de Privacidade Local relevante sobre sua incapacidade de cumprir. Tal informação do Membro das BCR ao seu Cliente deve ser fornecida sem demora e assim que o Membro das BCR tiver conhecimento de que a conformidade não é alcançável. Nesse caso, o Cliente terá o direito de suspender a transferência de Dados Pessoais para o Membro das BCR ou as atividades de Processamento em curso e/ou rescindir o contrato.

4.3 Qualidade dos Dados

Os Membros das BCR se comprometem a ajudar e assistir o Cliente a cumprir com a Legislação Aplicável em Proteção de Dados.

Em particular, os Membros das BCR auxiliarão seus Clientes para permitir que os Titulares de Dados exerçam seus direitos, realizando as medidas necessárias solicitadas pelos Clientes para atualizar, corrigir ou eliminar os Dados Pessoais, ou qualquer outro direito que o Titular de Dados possa exercer.

Nesse caso, o Membro das BCR informará cada Membro das BCR relevante (ou Afiliado da Concentrix não sujeito às BCR) para quem os Dados Pessoais tenham sido divulgados sobre qualquer correção, eliminação ou anonimização dos dados pessoais.

A pedido de seus Clientes e quando for viável, os Membros das BCR também implementarão medidas para eliminar ou anonimizar os Dados Pessoais no momento em que a forma identificável desses dados não for mais necessária.

4.4 Registro de atividades de processamento

Quando atuarem como Operadores, os Membros das BCR deverão manter um registro de todas as categorias de atividades de Processamento de Dados Pessoais realizadas em nome de um Controlador de Dados, que deve mencionar, pelo menos:

5. **O nome e os dados de contato dos Membros das BCR e do(s)**
6. **Controlador(es) de Dados em nome dos quais a Concentrix atua;**

7. **As categorias de processamento realizadas;**
8. **As possíveis transferências de Dados Pessoais para um país terceiro ou para uma organização internacional;**
9. **Uma descrição geral das medidas de segurança técnicas e organizacionais para garantir um nível de segurança adequado ao risco do processamento.**

9.1 Segurança

Quando atuarem como Encarregado dos Dados, os Membros das BCR se comprometem a cumprir todas as medidas técnicas e organizacionais adequadas para garantir um nível de segurança apropriado aos riscos apresentados pelo Tratamento, atendendo, no mínimo, aos requisitos da Legislação Aplicável em Proteção de Dados, e em particular ao artigo 32 do RGPD e a quaisquer medidas específicas estabelecidas no Acordo de Serviço com o Cliente.

Os Membros das BCR deverão notificar o Cliente sem demora indevida após tomarem conhecimento de uma violação de Dados Pessoais e deverão cumprir com o procedimento aplicável de Violação de Dados Pessoais adotado pelos Membros das BCR em cooperação com o Controlador de Dados.

9.2 Direitos dos Titulares de Dados

Os Membros das BCR se comprometem a executar as medidas necessárias solicitadas pelo Cliente e a fornecer qualquer informação útil para ajudar esse Cliente a cumprir com sua obrigação de observar os direitos dos Titulares de Dados, conforme detalhado na Seção 7 desta BCR-P.

Considerando a natureza do tratamento e as informações disponíveis para o Encarregado, os Membros das BCR fornecerão assistência e cooperação ao Cliente, na medida do possível e acordado com o Cliente, para o cumprimento da obrigação do Cliente de responder às solicitações. Os Membros das BCR seguirão o Procedimento para as solicitações dos Titulares de Dados quando atuarem como Encarregado dos Dados, anexado a esta BCR-P..

Quando um Membro das BCR receber uma solicitação do Titular dos Dados para exercer seus direitos, esse membro das BCR informará o cliente e este último responderá à solicitação. De acordo com a Legislação Aplicável em Proteção de Dados, o Cliente é responsável por gerenciar a solicitação. O membro das BCR será responsável apenas por seguir as Instruções adicionais de seu Cliente sobre como gerenciar essa solicitação e por cooperar com o Cliente para gerenciar essas solicitações.

9.3 Subprocessamento e transferências subsequentes

Os Membros das BCR ou fornecedores terceirizados podem subprocessar os Dados Pessoais de acordo com as disposições do Acordo de Serviço acordado com o Cliente. Os Subencarregados devem fornecer garantias suficientes para implementar as medidas técnicas e organizacionais adequadas, de forma que o Tratamento de Dados esteja em conformidade com os requisitos da Legislação Aplicável em Proteção de Dados, estas BCR-P e qualquer acordo de Tratamento de Dados aplicável.

Os Membros das BCR não utilizarão um Subencarregado sem primeiro obter uma autorização por escrito do Controlador. Ao conceder uma autorização geral para utilizar Subencarregados, o Membro das BCR correspondente informará o Cliente sobre qualquer mudança prevista em relação à adição ou substituição de Subencarregados qualquer Subencarregado e dará ao cliente a oportunidade de contestar essas mudanças e de rescindir o(s) formulário(s) de pedido aplicável(eis), conforme descrito abaixo e no Acordo de Serviço e no Acordo de Tratamento de Dados. Desde que os termos do Acordo de Serviço aplicável e do Acordo de Tratamento de Dados e/ou formulário(s) de pedido não privem o Controlador de Dados do direito de se opor ou de rescindir os serviços, o Controlador de Dados poderá, mediante notificação por escrito ao Membro das BCR correspondente, rescindir o(s) formulário(s) de pedido aplicável(eis) em relação aos Serviços que não possam ser prestados pelo Membro das BCR sem o uso do novo Subencarregado contestado.

O Subencarregado estará vinculado por meio de um contrato ou outro ato legal que exija que o referido Subencarregado cumpra com termos e obrigações que sejam pelo menos tão rigorosos e ofereçam pelo menos o mesmo nível de proteção que os descritos na Legislação de Proteção de Dados, nestas BCR-P e em um Acordo de Tratamento de Dados. O cliente poderá razoavelmente exigir que o Membro das BCR forneça a lista de Subencarregados autorizados para Processar Dados Pessoais. O contrato deverá especificar os propósitos do Tratamento, sua natureza, as categorias de Dados Pessoais Processados e as categorias de Titulares de Dados.

Em caso de uma obrigação legal de divulgar Dados Pessoais às autoridades competentes, os Membros das BCR envolvidos devem notificar a Webhelp SAS e o DPO. A Webhelp SAS se compromete a notificar a Autoridade de Supervisão relevante do EEE e, a menos que seja proibido de outra forma, ao Cliente sobre essa divulgação sem demora indevida e a cumprir com o princípio de minimização de Dados. O Membro das BCR deverá especificar quais Titulares de Dados estão afetados pela divulgação, qual autoridade está solicitando essa divulgação e qual base legal está sendo utilizada. Em qualquer caso, os Membros das BCR se comprometem a não transferir Dados Pessoais para as autoridades públicas de maneira maciça e desproporcional. Nesse mesmo caso, os Membros das BCR se comprometem a notificar o Cliente sobre a divulgação. Qualquer notificação a um Membro das BCR e a notificação planejada às Autoridades de Supervisão do EEE estão sujeitas ao mecanismo e às disposições do Artigo 13.3 abaixo.

Além disso, cada Membro das BCR deverá garantir e verificar que todos os seus Subencarregados e, em particular, qualquer outro Membro das BCR envolvido no Tratamento de Dados Pessoais, tenham sido devidamente aprovados pelo Cliente, seja por meio de uma autorização geral ou específica por escrito.

10. Tratamento de dados sensíveis

Os Membros das BCR se comprometem a cumprir com as disposições do Artigo 4 – Princípios para o Tratamento de Dados Pessoais e reconhecem que os Dados Pessoais Sensíveis requerem a implementação de uma proteção específica, uma vez que tais Dados Pessoais podem criar riscos significativos em relação aos direitos e liberdades fundamentais do Titular dos Dados.

Quando os Membros das BCR forem solicitados por seu Cliente para Processar Dados Pessoais Sensíveis, os Membros das BCR podem ser exigidos a implementar medidas e controles de segurança adicionais, técnicos, físicos e administrativos.

Será responsabilidade do Cliente dos Membros das BCR definir quais medidas devem ser implementadas nesse aspecto e garantir que os requisitos da Legislação Aplicável em Proteção de Dados sejam cumpridos e, quando pertinente, de qualquer outro framework setorial aplicável adotado pelas Autoridades de Supervisão do EEE.

Para maior clareza, quando Dados Pessoais Sensíveis forem Processados como Encarregados de Dados, os Membros das BCR não serão, em hipótese alguma, responsáveis por garantir que o Tratamento se baseie em uma das bases legais definidas no Artigo 4 mencionado anteriormente – Princípios para o Tratamento de Dados Pessoais.

11. Transferência de Dados Pessoais para países terceiros e restrição da Transferência subsequente para Membros que não sejam das BCR

11.1 Transferências e Transferências Subsequentes de Dados Pessoais

No decorrer de suas atividades, os Membros das BCR podem processar Dados Pessoais em nome de seu(s) Cliente(s). Esses Membros das BCR ou Cliente(s) podem estar localizados fora do Espaço Econômico Europeu (a seguir, 'EEE'), e, portanto, implicar Transferências de Dados Pessoais. Nesse caso, estas BCR-P se aplicam a:

- Dados Pessoais recebidos de um Cliente que atua como Controlador de Dados e está localizado dentro do EEE, que são então processados pelos Membros das BCR, atuando como Encarregados do Tratamento em nome desse Cliente; e

- Transferências de Dados Pessoais de um Membro das BCR atuando como Encarregado do Tratamento em nome de um Cliente e localizado dentro do EEE para outro Membro das BCR fora do EEE, atuando como Encarregado de dados.

Caso contrário, quando os Dados Pessoais forem transferidos, a Concentrix implementará garantias específicas para assegurar que os Dados Pessoais transferidos tenham um nível adequado de proteção, conforme detalhado a seguir:

- Transferências de Dados Pessoais de um Membro das BCR que atue como Encarregado de Dados para um Afiliado da Concentrix (não sujeito às BCR-P) ou para terceiros localizados fora do EEE (mais especificamente em um país não pertencente ao EEE que tenha recebido uma decisão de adequação por parte da Comissão da UE) e que atue como Encarregado dos Dados serão respaldadas por um acordo escrito que inclua as cláusulas Contratuais Padrão aplicáveis adotadas pela Autoridade de Supervisão competente do EEE e/ou pela Comissão da UE (como as SCCs da Comissão da UE sobre Transferências (914/2021), Módulo 3 Encarregado a Encarregado), desde que o Encarregado dos Dados tenha permitido à Concentrix proceder com tal transferência em seu nome, incluindo qualquer transferência subsequente; ou;
- Transferências de Dados Pessoais de um Membro das BCR que atue como Encarregado dos Dados para um Afiliado da Concentrix (não sujeito às BCR-P) ou para terceiros localizados fora do EEE (mais especificamente em um país não pertencente ao EEE que tenha recebido uma decisão de adequação por parte da Comissão da UE) como Encarregado dos Dados serão respaldadas por um acordo escrito que inclua as cláusulas contratuais padrão aplicáveis adotadas pela Autoridade de Supervisão competente do EEE e/ou pela Comissão da UE (como as SCCs da Comissão da UE sobre Transferências (914/2021), Módulo 4 Encarregado a Controlador), desde que o Controlador dos Dados tenha permitido à Concentrix proceder com tal transferência em seu nome, incluindo qualquer transferência subsequente.
- Na ausência de uma decisão de adequação ou de salvaguardas apropriadas conforme descrito anteriormente, as transferências podem ser realizadas excepcionalmente se uma exceção prevista no Artigo 49 do RGPD se aplicar e devem ser ocasionais e não repetitivas.

Em qualquer caso, os Membros das BCR que atuem como Encarregado dos Dados se comprometem a não transferir Dados Pessoais para terceiros que não façam

parte do Grupo Concentrix sem garantir previamente que será oferecido um nível adequado de proteção para os Dados Pessoais transferidos, de acordo com o RGPD, de forma que o nível de proteção do titular dos Dados seja assegurado e não comprometido.

Para maior clareza, quando um Membro das BCR atuar como Encarregado dos Dados, somente procederá com a Transferência com base em instruções documentadas do Controlador dos Dados, a menos que seja obrigado a fazê-lo pela legislação da União ou do Estado Membro ao qual o Membro das BCR esteja sujeito. Nesse caso, o Membro das BCR deverá informar o Controlador dos Dados sobre tal requerimento legal antes de Processar os Dados Pessoais, a menos que tal lei proíba essa informação por razões de interesse público importante reconhecidas na legislação da União ou na legislação do Estado Membro ao qual o Controlador dos dados estejam sujeito.

11.2 Obrigação do Importador dos Dados em caso de solicitação de acesso por parte do governo

Sem prejuízo da obrigação do Membro das BCR que atua como Importador dos Dados de informar ao Exportador dos Dados sobre sua incapacidade de cumprir com os compromissos contidos nas BCR-P (Artigo 13.3 abaixo), o Membro das BCR que atua como Importador dos Dados notificará imediatamente ao Exportador dos Dados e, quando possível, ao Titular dos Dados (se necessário, com a ajuda do Exportador dos Dados) se:

- Receber uma solicitação legalmente vinculante de uma autoridade sob as leis do país de destino, ou de outro país terceiro, para a divulgação de Dados Pessoais transferidos de acordo com as BCR-P. Tal notificação incluirá informações sobre os Dados Pessoais solicitados, a autoridade solicitante, a base legal da solicitação e a resposta fornecida;
- Tomar conhecimento de qualquer acesso direto por parte de autoridades aos Dados Pessoais transferidos de acordo com as BCR-P, conforme as leis do país de destino. Tal notificação incluirá todas as informações disponíveis para o Importador dos Dados.

Se for proibido notificar o Exportador dos Dados e/ou o Titular dos Dados, o Importador dos Dados fará o possível para obter uma isenção dessa proibição, com o objetivo de comunicar a maior quantidade de informação possível e o mais rápido possível, e documentará seus melhores esforços para poder comprová-los mediante solicitação do Exportador dos Dados.

O Importador dos Dados fornecerá ao Membro das BCR que atua como Exportador dos Dados, em intervalos regulares, a maior quantidade de informação relevante possível sobre as solicitações recebidas (em particular, o número de solicitações, o tipo de dados solicitados, a autoridade ou autoridades solicitantes, se as solicitações foram contestadas e o resultado dessas contestações, etc.). Se ao Importador dos Dados for proibido parcial ou totalmente fornecer ao Exportador dos Dados as informações mencionadas anteriormente, ele informará o Exportador dos Dados sem demora indevida.

O Importador dos Dados manterá as informações mencionadas anteriormente enquanto os Dados Pessoais estiverem sujeitos às Salvaguardas fornecidas pelas

BCR-P, e as disponibilizará à Autoridade de Supervisão Competente quando solicitado.

O Importador dos Dados revisará a legalidade da solicitação de divulgação, particularmente se ela está dentro das faculdades concedidas à autoridade solicitante, e contestará a solicitação se, após uma avaliação minuciosa, concluir que existem razões fundamentadas para considerar que a solicitação é ilegal conforme as leis do país de destino, as obrigações aplicáveis sob o direito internacional e os princípios de cortesia internacional.

O Importador dos Dados, sob as mesmas condições, buscará as possibilidades de apelação.

Ao contestar uma solicitação, o Importador dos Dados buscará medidas cautelares com o objetivo de suspender os efeitos da solicitação até que a autoridade judicial competente se pronuncie sobre o mérito da questão. Não divulgará os Dados Pessoais solicitados até que seja obrigado a fazê-lo conforme as normas processuais aplicáveis.

O Importador dos Dados documentará sua avaliação legal e qualquer contestação à solicitação de divulgação e, na medida em que as leis do país de destino permitirem, disponibilizará a documentação ao Exportador dos Dados. Também a disponibilizará à Autoridade de Supervisão Competente quando solicitado.

O Importador dos Dados fornecerá a menor quantidade de informação permitida ao responder a uma solicitação de divulgação, com base em uma interpretação razoável da solicitação.

Em qualquer caso, as Transferências de Dados Pessoais por um Membro das BCR a qualquer autoridade pública não podem ser massivas, desproporcionais ou indiscriminadas, de maneira a exceder o necessário em uma sociedade democrática (ver Artigo 12.3 das BCR-P sobre o assunto).

12. Direitos do Titular dos Dados

12.1 Direitos de Beneficiário de Terceiros

Quando um Membro das BCR atuar como Encargado dos Dados em nome de seus Clientes, os Titulares dos Dados poderão exercer seus direitos em relação ao Processamento de seus Dados Pessoais diretamente contra os Clientes Membros das BCR.

No entanto, quando a solicitação dos Titulares dos Dados se referir a requisitos impostos aos Processadores de Dados, os Titulares dos Dados deverão fazer valer pelo menos os seguintes direitos diretamente contra os Membros das BCR:

- Dever de respeitar as instruções do responsável pelos Dados em relação ao Processamento de Dados Pessoais, incluindo para as Transferências de Dados Pessoais para países terceiros (Artigos 4.2 e 6).
- Dever de implementar medidas de segurança técnicas e organizativas apropriadas e deve notificar qualquer Incidente de Violação de Dados Pessoais ao Responsável pelos Dados (Artigos 4.5, 4.7 e 3).

- Dever de cumprir com as condições ao contratar um Sub-Encargado que os Membros das BCR estabeleçam (Artigo 4.7).
- Dever de cooperar e auxiliar o Responsável pelos Dados no cumprimento e na demonstração de conformidade com a lei, como na resposta a solicitações dos Titulares dos Dados em relação aos seus direitos (Artigos 4.6 e 4.7).
- Acesso fácil às BCR-P no site da Concentrix (atualmente em www.concentrix.com);
- Direito de apresentar queixas através de mecanismos internos de reclamação (Artigo 8);
- Dever de cooperar com o Órgão de Vigilância do EEE (Artigo 13.4);
- Disposições sobre responsabilidade, compensação e jurisdição (Artigo 9);
- Legislação nacional que impeça o cumprimento das BCR-P (Artigos 4.1, 6.2 e 13.3);
- Dever de garantir a exigibilidade dos direitos de terceiros beneficiários (Artigo 7).

Em qualquer caso, os Titulares dos Dados:

- Têm o direito de buscar recursos judiciais por qualquer descumprimento dos direitos garantidos por estas BCR-P e/ou pela Legislação de Proteção de Dados Aplicável (Artigo 9);
- Têm o direito de obter reparação e, quando apropriado, receber compensação por danos (incluindo danos materiais, bem como qualquer sofrimento) resultantes da violação das BCR-P por qualquer Membro das BCR (Artigo 9);
- Têm o direito de apresentar uma queixa perante o Órgão de Vigilância do EEE ou perante os tribunais competentes para o Cliente localizado no EEE (Artigos 7.1 e 7.2).

Sem prejuízo de outros recursos da Concentrix, quando o Responsável pelo Tratamento e o Controlador de Dados envolvidos no mesmo Tratamento forem responsáveis por qualquer dano causado por tal Tratamento, o Titular dos Dados terá o direito de receber uma compensação total pelo dano diretamente do Membro das BCR que atue como Encargado do Tratamento.

Caso se possa evidenciar que o Cliente desapareceu ou não existe mais legalmente ou se tornou insolvente e nenhuma outra entidade assumiu as obrigações legais de recuperar as obrigações do Cliente, os Titulares dos Dados têm expressamente o direito de exercer os seguintes direitos e apresentar uma reclamação direta contra o Membro das BCR que atue como Encargado do Tratamento e esteja vinculado por um Acordo de Serviço com o Cliente:

- Obrigação de cumprir os elementos executáveis das BCR-P (artigos 3.1 e 3.2);
- Dever de garantir a exigibilidade dos direitos dos terceiros beneficiários (artigo 7);
- A aprovação por parte da Webhelp SAS de i) a responsabilidade de pagar indenizações e de remediar qualquer descumprimento das BCR-P por parte

de um Membro das BCR localizado fora do EEE que resulte em danos recuperáveis, assim como ii) a responsabilidade de demonstrar que o Membro das BCR relevante não é responsável pela alegada violação das BCR-P que resultou nos danos reclamados pelo Titular dos Dados (artigo 7.2)

- Acesso fácil às BCR-P no site da Concentrix (atualmente em www.concentrix.com);
- Direito de apresentar uma queixa através do mecanismo interno de queixas das empresas (Anexo 5 – Artigo 3.1);
- Deveres de cooperação com o Órgão de Vigilância do EEE (Artigo 13.4);
- Dever de cooperar com o Responsável pelos Dados (Artigo 4.1);
- Dever de cumprir com os princípios para o Tratamento de Dados Pessoais estabelecidos no Artigo 4;
- Disponibilizar e atualizar a lista de entidades sujeitas às BCR (Anexo 1); e
- Legislação nacional que impede o cumprimento das BCR-P (Artigo 13.3);

Um Membro das BCR aceita que os Titulares de Dados podem ser representados por uma entidade, organização ou associação sem fins lucrativos para apresentar a queixa em seu nome e exercer os direitos acima mencionados. Tal entidade, organização ou associação deve estar devidamente constituída pela legislação de um Estado Membro, ter objetivos estatutários de interesse público e estar ativa na proteção dos direitos e liberdades dos Titulares de Dados em relação à segurança de seus Dados Pessoais.

Para maior clareza, especifica-se que os direitos de terceiros beneficiários descritos anteriormente não se estendem aos elementos das BCR-P relacionados com mecanismos internos implantados nas entidades, como detalhes de formação, programa de auditoria, rede de conformidade e mecanismo de atualização das BCR-P.

Considere que, sem prejuízo do disposto no presente artigo 7, a Concentrix incentiva os Titulares de Dados a utilizarem o mecanismo interno de reclamação descrito no artigo 8 das BCR-C, que se encontra a seguir.

13. Direito de reclamar e obter reparação judicial, compensação e indenização quando um membro das BCR fora do EEE não cumprir com as BCR-P

14. o caso de um membro das BCR fora do EEE não cumprir com as BCR-P, a Webhelp SAS (1) assume a responsabilidade por qualquer dano resultante do descumprimento das BCR-P, incluindo o pagamento de uma indenização quando concedida pelo tribunal competente e

(2) compromete-se a tomar as medidas necessárias para remediar os atos desse outro membro das BCR.

Nessas circunstâncias, a Webhelp SAS também reconhece que o Titular dos Dados terá direito a:

- apresentar uma denúncia perante um Órgão de Vigilância do local onde resida, trabalhe ou onde esteja estabelecido o Membro das BCR com responsabilidade delegada; e/ou;
- um recurso judicial efetivo quando o Titular dos Dados considerar que o Tratamento de Dados Pessoais que o afeta, realizado por qualquer Membro das BCR que atue como Encarregado do Tratamento, infringe as presentes BCR-P. Os Membros das BCR reconhecem que tal reclamação pode ser feita perante o Estado-membro no qual o Membro das BCR responsável pelo descumprimento está estabelecido ou perante o tribunal no qual o Titular dos Dados tenha sua residência habitual.

A Webhelp SAS será responsável por demonstrar que o referido membro das BCR fora do EEE não é responsável por nenhuma violação das regras especificadas nas presentes BCR-P que tenha resultado em reclamação de danos por parte do Titular dos Dados. Caso a Webhelp SAS consiga demonstrar que o outro membro das BCR localizado fora do EEE não foi responsável pelo ato, poderá isentar-se de qualquer responsabilidade.

Quando o Responsável puder demonstrar que sofreu danos e apresentar provas de que os danos provavelmente ocorreram devido a uma violação dessas BCR-P por parte de um Membro das BCR fora do EEE, a Webhelp SAS será responsável por demonstrar que o Membro das BCR fora do EEE ou o Subencarregado externo fora do EEE não foi responsável pela violação das BCR-P que deu origem aos danos em questão ou que tal violação não ocorreu.

14.1 Direitos dos Titulares dos Dados

Os Titulares dos Dados têm o direito de usufruir dos seguintes direitos:

- Ter acesso aos Dados Pessoais que lhe dizem respeito e que são tratados por um membro das BCR.
- Solicitar a retificação ou eliminação de qualquer Dado Pessoal impreciso ou incompleto que lhe diga respeito, bem como de qualquer Dado Pessoal cujo tratamento não seja mais lícito ou adequado; ou seja:
- Solicitar que o tratamento de seus Dados Pessoais seja limitado.
- Opor-se ao tratamento dos Dados dos Titulares por parte de um membro das BCR quando tal tratamento for necessário para os fins dos interesses legítimos perseguidos pelo Responsável pelos Dados, para fins de interesses legítimos, incluindo a elaboração de perfis, em qualquer momento, por motivos

relacionados com sua situação pessoal, a menos que os interesses perseguidos pelo Cliente, atuando como Responsável pelos Dados, prevaleçam sobre os interesses, direitos e liberdades dos Titulares dos Dados.

- Opor-se ao tratamento dos Dados dos Titulares por parte de um membro das BCR quando tal tratamento for necessário para os fins dos interesses legítimos perseguidos pelo Responsável pelos Dados ou por um terceiro, para fins de marketing, incluindo a elaboração de perfis; e
- Receber seus Dados Pessoais em um formato estruturado, de uso comum, legível por máquina e interoperável quando o tratamento for realizado por meios automatizados.

Quando um membro das BCR atuar como Encarregado dos Dados e receber uma solicitação dos Titulares dos Dados para exercer seus direitos, o membro das BCR deverá informar ao seu Cliente, e este último deverá responder à solicitação. Um membro das BCR será responsável apenas por seguir as instruções adicionais de seu Cliente sobre como lidar com tal solicitação. Os membros das BCR executarão qualquer medida necessária solicitada pelo Cliente para que os Dados Pessoais sejam atualizados, corrigidos, eliminados ou anonimizados a partir do momento em que o formulário de identificação já não for necessário. Os membros das BCR deverão comunicar essas instruções a qualquer membro relevante das BCR para quem os Dados Pessoais tenham sido divulgados. Os membros das BCR também executarão as medidas técnicas e organizativas apropriadas, na medida do possível, seguindo as instruções do Cliente, para cumprir sua obrigação de responder às solicitações, incluindo a comunicação de qualquer informação útil. Quando o Cliente tiver desaparecido, deixado de existir ou se tornado insolvente, o membro relevante das BCR deverá lidar diretamente com tal solicitação na medida do possível e de acordo com o procedimento que tenha adotado.

14.2 Exercício dos Direitos dos Titulares dos Dados

Os Titulares dos Dados têm o direito de fazer cumprir essas BCR-P como beneficiários de terceiros e de exercer seus direitos em relação ao Tratamento dos Dados pelos Titulares por qualquer membro das BCR que atue como Encarregado dos Dados. O membro das BCR deve garantir que qualquer solicitação ou reclamação dos Titulares dos Dados relacionada ao exercício de seus direitos (“Solicitações”) seja tratada de maneira oportuna.

Os Titulares dos Dados podem fazer uma solicitação verbalmente ou por escrito. Os membros das BCR fornecerão aos Titulares dos Dados meios acessíveis para exercer seus direitos e, em particular:

1 - Um e-mail de contato único que será utilizado independentemente do país em que o Titular dos Dados se encontre:

dpo@concentrix.com

Podem ser utilizados e-mails locais para levar em consideração especificidades locais, como o idioma.

Para entrar em contato com seu contato local de privacidade, consulte o Apêndice 01 - Lista de entidades da Concentrix obrigadas pelo BCR-P e contatos locais de privacidade por e-mail.

2 - Portal único com o endereço de e-mail do DPO da Concentrix acessível através de um link em www.concentrix.com

3 - Endereço postal único que será utilizado independentemente do país em que o Titular dos Dados se encontre:

Group Data Privacy Officer

Legal and Compliance Department

3 rue d'Heliopolis

75017 – PARIS

FRANÇA

O DPO, ou qualquer outra pessoa ou entidade, interna ou externa, designada pelo DPO para gerenciar as Solicitações, deverá (i) garantir que tenha obtido as informações mínimas necessárias do Titular dos Dados para tratar sua Solicitação e (ii), se considerado necessário, obter o maior número possível de informações para que a Solicitação seja gerida adequadamente.

Se houver dúvidas sobre a identidade da pessoa que faz a solicitação, principalmente quando são utilizados meios de comunicação à distância, um membro das BCR pode solicitar mais informações sobre o Titular dos Dados. As informações coletadas deverão (i) limitar-se às informações necessárias para confirmar a identidade da pessoa que faz a solicitação e (ii) não devem ser coletadas quando os produtos ou serviços fornecidos por um membro das BCR ou seus Clientes não são entregues sob a identidade real do usuário. A proporcionalidade será sempre avaliada pelo Responsável pelos Dados.

Em qualquer caso, a resposta ao Titular dos Dados deve ocorrer dentro de um prazo máximo de 1 mês após o recebimento da Solicitação. Considerando a complexidade e o número de solicitações, esse prazo pode ser estendido por no máximo dois meses adicionais, caso em que o reclamante deve ser informado em consequência (conforme detalhado no Apêndice 6).

Quando o Titular dos Dados não estiver satisfeito com a resposta inicial fornecida pelo membro das BCR, o Titular dos Dados terá o direito de solicitar imediatamente que sua Solicitação seja reconsiderada. O Titular dos Dados deverá fornecer ao membro das BCR uma explicação detalhada das disposições insatisfatórias da solução previamente fornecida. O membro das BCR não deverá levar mais de 2 meses desde o recebimento da Solicitação de reconsideração para determinar como será tratada e deverá informar o Titular dos Dados por escrito em consequência.

Se uma Solicitação ou reclamação do Titular dos Dados for rejeitada pelo membro das BCR ou se a resposta não satisfizer o Titular dos Dados, o Titular dos Dados poderá entrar em contato com o DPO e/ou apresentar uma reclamação diretamente a um Órgão de Vigilância competente do EEE e/ou buscar uma via judicial.

Detalhes adicionais sobre este Artigo estão disponíveis no seguinte apêndice:

- **Apêndice 6 - Procedimento para as solicitações dos Titulares dos Dados quando a Concentrix atua como Encarregado dos Dados.**

15. Processo para o manejo de denúncias dos Titulares dos Dados

Quando o Titular da Informação comunicar uma reclamação diretamente a um Membro das BCR, mas o cliente não tiver deixado de existir, não tiver desaparecido ou não tiver se tornado insolvente no momento em que tal solicitação for recebida pelo Membro das BCR, então o Membro das BCR compromete-se a informar o cliente sobre tal solicitação sem demora e de acordo com o procedimento definido no **Apêndice 6 – Procedimento para as solicitações dos Titulares da Informação quando a Concentrix atua como o Encarregado dos Dados**

Nesse caso, o Membro das BCR compromete-se a comunicar qualquer informação relevante que receba do Titular da Informação ao Cliente, e concorda em indicar expressamente ao Cliente que é responsabilidade do Cliente gerenciar tal reclamação.

A Concentrix não é responsável pelo manejo de reclamações feitas pelos Titulares da Informação quando atua como Encarregado dos Dados. No entanto, caso o cliente tenha desaparecido de fato, deixado de existir de acordo com a lei ou tenha sido declarado insolvente, os Membros das BCR comprometem-se a gerenciar as reclamações dos Titulares da Informação de acordo com o mesmo procedimento especificado no Artigo 8 das BCR-P. Nesse caso, os Membros das BCR reconhecem que os Titulares da Informação ainda têm o direito de apresentar uma reclamação a um Órgão de Vigilância do EEE e/ou buscar recursos judiciais. Os Membros das BCR também reconhecem que esses direitos não dependem de os Titulares da Informação terem utilizado previamente o processo para o manejo de reclamações, no entanto, é incentivado que os Titulares da Informação o façam.

16. Reclamações de Clientes Externos

Quando um membro das BCR que atue como Encarregado dos Dados não cumprir com essas BCR-P, a Concentrix reconhece que o Cliente tem o direito de fazer cumprir essas BCR-P contra um Membro das BCR que não as esteja cumprindo.

O Cliente terá o direito a recursos judiciais e a receber compensação do Membro das BCR que tenha causado a violação, conforme o estipulado no Acordo de Serviço e/ou no Acordo de Processamento de Dados.

17. Governança de proteção de dados

A Concentrix definiu uma organização e governança de proteção de dados, a qual é detalhada no Apêndice 3.

Os membros das BCR comprometem-se a designar um Oficial de Privacidade de Dados, quando necessário e em conformidade com o Artigo 37 do RGPD, ou qualquer outra pessoa ou entidade (como o responsável pela privacidade) com a responsabilidade de monitorar o cumprimento das BCR-P e que tenha o mais alto apoio administrativo para o cumprimento desta tarefa. Esta organização é liderada pelo Oficial de Privacidade do Grupo, que conta com uma rede de pontos de contato de privacidade (especificamente os Líderes Regionais de Privacidade, Líderes Locais de Privacidade, além dos Referentes de Privacidade do Negócio) e que podem ser designados como DPO pelo membro competente das BCR.

O DPO nomeado formalmente junto a um Órgão de Vigilância deve reportar-se diretamente ao nível mais alto da administração. Adicionalmente, o DPO pode informar o nível mais alto da administração se surgir qualquer dúvida ou problema durante o exercício de suas funções.

O DPO não deve ter tarefas que possam resultar em conflitos de interesse. O DPO não deve ser responsável por realizar avaliações de impacto sobre a proteção de dados, nem por realizar auditorias das BCR se isso resultar em um conflito de interesses. No entanto, o DPO pode desempenhar um papel muito útil e importante ao assistir os membros das BCR, e sugestões do DPO devem ser solicitadas.

Os papéis e responsabilidades da rede, bem como sua governança de trabalho, são definidos em detalhes no **Apêndice 3 – Organização e governança da proteção de dados.**

Adicionalmente, o DPO pode informar o nível mais alto da administração se surgirem dúvidas ou problemas durante o exercício de suas funções.

O DPO e os Líderes Locais e Regionais de Privacidade podem ser contatados através das informações de contato descritas no Artigo 7.5 das BCR-C e nos contatos de privacidade locais fornecidos no Apêndice 01 das BCR.

18. Treinamento e conscientização

Proteger os Dados Pessoais não é apenas uma questão de cumprir as leis de privacidade, mas também faz parte da materialização dos valores fundamentais da Concentrix. Nesse contexto, promover uma cultura de privacidade dentro do grupo é essencial para garantir que todos os funcionários, estagiários e outras pessoas cujas condutas no exercício de suas funções estejam sob o controle direto dos Membros das BCR sejam responsáveis pela proteção dos Dados Pessoais processados como parte de suas operações.

Portanto, essas BCR-P devem ser implementadas adequadamente em toda a organização. Para isso, os Membros das BCR adotaram um programa de treinamento em privacidade, com o objetivo de garantir que os funcionários da Concentrix, estagiários e outras pessoas cuja conduta, no exercício de suas funções, esteja sob o controle direto dos Membros das BCR, estejam realmente cientes das obrigações, princípios e procedimentos especificados nessas BCR-P. Além dos princípios e obrigações principais do RGPD, o programa de treinamento e

conscientização deve cobrir, entre outros, os procedimentos para lidar com solicitações de acesso a informações pessoais por parte das autoridades públicas.

Esse treinamento é dirigido a: (i) pessoas que tenham acesso permanente ou regular aos Dados Pessoais; (ii) pessoas envolvidas na coleta de Dados Pessoais; e/ou (iii) pessoas envolvidas no desenvolvimento de ferramentas usadas para processar Dados Pessoais.

O material de capacitação deve estar atualizado e revisado periodicamente, pelo menos uma vez por ano ou quando ocorrerem mudanças significativas na legislação de proteção de dados aplicável, a fim de garantir que reflita a versão mais recente das BCR-P.

O programa de treinamento visa proporcionar:

- Um nível básico de conhecimento fundamental dos princípios que se aplicam ao processar os Dados Pessoais e um bom conhecimento dos processos existentes e sua implementação, e
- Treinamento específico adaptado às diferentes funções dentro da organização.

Neste sentido, é lembrado que os Membros das BCR reconhecem que nenhuma transferência pode ser feita sob as BCR-P para outro Membro das BCR, a menos que este último esteja efetivamente vinculado pelas BCR-P e que um treinamento efetivo sobre as BCR-P possa ser proporcionado aos funcionários do respectivo Membro das BCR.

Os Membros das BCR comprometem-se a garantir que todos os funcionários da Concentrix, seus estagiários e outras pessoas cujas condutas, no exercício de seu trabalho, estejam sob o controle direto dos Membros das BCR, participem do treinamento assim que esteja disponível e, posteriormente, completem o curso de atualização anual.

Mais detalhes sobre este artigo estão disponíveis no seguinte apêndice:

- **Apêndice 04 – Programa de treinamento e conscientização.**

19. Privacidade por design / privacidade por padrão

Quando atuarem como Encarregados dos Dados, os Membros das BCR devem seguir qualquer instrução razoável do Cliente para permitir que este último cumpra com suas obrigações relacionadas à Privacidade por design e à Privacidade por padrão.

20. Transparência e Cooperação

20.1 Comunicação das BCR-P

Os Membros das BCR comprometem-se a garantir que todos os Titulares dos Dados recebam informações sobre seus direitos como beneficiários terceiros em relação ao processamento de seus Dados Pessoais, bem como sobre os meios para exercer esses direitos. Essas informações estão descritas no Artigo 7 das BCR-P.

A Concentrix comunicará abertamente essas BCR-P aos Titulares dos Dados e as tornará facilmente acessíveis a qualquer pessoa. Essa comunicação deve permitir que qualquer Titular dos Dados obtenha uma cópia dessas BCR-P sem atrasos injustificados e em um formato aberto.

Adicionalmente, uma versão pública da versão mais recente das BCR-P deve estar disponível a qualquer momento para os Titulares dos Dados no site da Concentrix, www.concentrix.com. Os Titulares dos Dados também podem solicitar uma cópia das BCR-P entrando em contato com o DPO em dpo@concentrix.com.

A versão pública das BCR-P deve conter, pelo menos, as seguintes informações:

- Uma descrição do escopo das BCR-P (Artigo 2 das BCR-P), · A cláusula relacionada às responsabilidades do Grupo (Artigo 7 das BCR-P), · As cláusulas relacionadas aos princípios de proteção de dados (Artigos 4 e 5 das BCR-P),
- Notificações de segurança e de violações de informações pessoais (Artigo 4.5 das BCR-P),
- Subencarregados e restrições em transferências subsequentes (Artigos 4.7 e 6 das BCR-P), e · As cláusulas relacionadas aos direitos dos Titulares dos Dados (Artigos 7, 8 e 13 das BCR-P).

Essas informações devem ser atualizadas e apresentadas aos Titulares dos Dados de forma clara, inteligível e transparente. As informações devem ser fornecidas de forma completa; portanto, um resumo deste documento não será suficiente.

A versão pública também deve incluir todas as políticas e procedimentos exigidos anexos às BCR-P como Apêndice, especialmente para as BCR-P:

- Apêndice 01 – A Lista de Membros das BCR vinculados pelas BCR-P e os e-mails de contato de privacidade local
- Apêndice 02 – Definições para as BCR e procedimentos
- Apêndice 06 – Procedimento para as solicitações dos Titulares dos Dados onde a Concentrix atua como Encarregado dos Dados.
- Apêndice 11-B – Alcance material das BCR-P: Lista de finalidades do processamento e categorias relacionadas com os Dados Pessoais e os Titulares dos Dados.

Os outros Apêndices ou não são aplicáveis às BCR-C ou são processos internos irrelevantes para que os Titulares dos Dados entendam ou exerçam seus direitos.

Esses requisitos serão atendidos garantindo que a versão pública simplificada das BCR-P, que contém todas as informações listadas anteriormente, esteja disponível no site da Concentrix (www.concentrix.com).

Quando atuarem como Encarregados dos Dados, os membros das BCR comprometem-se a compartilhar essas BCR-P com seus clientes e a incluir essas BCR-P no Acordo de Serviço para divulgar e fazer cumprir as BCR-P. Em qualquer caso, quando atuarem como Encarregados dos Dados, conforme mencionado nos

Artigos 3 e 4 desta BCR-P, os membros das BCR comprometem-se a cumprir as BCR-P em relação ao Processamento dos Dados Pessoais de seu Cliente.

20.2 Informações aos Titulares dos Dados

Quando atuarem como Encarregados dos Dados, os Membros das BCR são responsáveis por fornecer a seus Clientes as informações pertinentes que lhes permitam facilitar aos Titulares dos Dados as informações relevantes exigidas pela Legislação Aplicável sobre Proteção de Dados.

No entanto, os Membros das BCR não serão responsáveis por fornecer as informações obrigatórias aos Titulares dos Dados conforme exigido pela Legislação Aplicável sobre Proteção de Dados, uma vez que os Clientes dos Membros das BCR são os únicos responsáveis a esse respeito.

20.3 Inconsistências com a legislação e práticas locais que afetam o cumprimento das BCR-P

Os membros das BCR comprometem-se a utilizar as BCR-P como ferramenta para as transferências somente quando tiverem avaliado que a legislação e as práticas de um País Terceiro Não Adequado aplicáveis ao tratamento dos dados pessoais pelo membro das BCR que atua como Importador dos Dados, incluindo qualquer requisito de revelação de dados pessoais ou medidas que autorizem o acesso das autoridades públicas, não impedem o cumprimento de suas obrigações sob estas BCR-P.

Esse compromisso baseia-se na compreensão de que as leis e práticas – que respeitam a essência dos direitos e liberdades fundamentais, e não excedem o que é necessário e proporcionado em uma sociedade democrática para salvaguardar um dos fins enumerados abaixo – não estão em contradição com as BCR-P:

(ee) segurança nacional, e/ou,
(ff) defesa, e/ou
(gg) segurança pública, e/ou
(hh) prevenção, investigação, detecção ou processamento de crimes ou execução de penas criminais, incluindo a proteção e prevenção de ameaças à segurança pública; e/ou
(ii) outros objetivos importantes de interesse público geral da União ou de um Estado-Membro, em particular um interesse econômico ou financeiro importante da União ou de um Estado-Membro, incluindo questões monetárias, orçamentárias e fiscais, saúde pública e segurança social; e/ou
(jj) a proteção da independência judicial e dos procedimentos judiciais; e/ou
(kk) a prevenção, investigação, detecção e processamento judicial das violações das normas éticas das profissões regulamentadas; e/ou
(ll) uma função de controle, inspeção ou regulamentação vinculada, mesmo que ocasionalmente, ao exercício do poder público nos casos contemplados nas letras a) a e) e g); e/ou

(mm) a proteção do Titular dos dados ou dos direitos e liberdades de terceiros; e/ou
(nn) a execução de reclamações de direito civil.

Na avaliação das leis e práticas do País Terceiro Não Adequado que possam afetar o respeito pelos compromissos contidos nas BCR-P, os Membros das BCR deverão levar em conta, em particular, os seguintes elementos:

- **As circunstâncias específicas das Transferências** ou conjunto de transferências, e de qualquer transferência subsequente prevista dentro do mesmo país terceiro ou para outro País Terceiro Não Adequado, incluindo:

  - fins para os quais os Dados Pessoais são transferidos e tratados (por exemplo, armazenamento, suporte de TI, serviços de terceirização de processos empresariais como atendimento ao cliente em nome do Cliente);
  - tipos de entidades envolvidas no Tratamento (o Importador dos Dados e qualquer outro destinatário de qualquer Transferência ulterior);
  - setor econômico no qual ocorre a Transferência ou conjunto de Transferências;
  - categorias e formato dos Dados Pessoais Transferidos;
  - local do tratamento, incluindo armazenamento; e
  - canais de transmissão utilizados.

- **As leis e práticas do País Terceiro de destino** relevantes à luz das circunstâncias da Transferência, incluindo aquelas que exigem a revelação de dados às autoridades ou autorizam o acesso dessas autoridades, e as que fornecem acesso a esses Dados Pessoais durante o trânsito entre o país do Exportador dos Dados e o país do Importador dos Dados, assim como as limitações e salvaguardas aplicáveis.
-
- **Todas as salvaguardas contratuais, técnicas ou organizacionais relevantes** estabelecidas para complementar as salvaguardas sob as BCR-P, incluindo as medidas aplicadas durante a transmissão e o Tratamento dos Dados Pessoais no país de destino.

Tendo em vista o exposto, quando um membro das BCR tiver motivos para acreditar que a legislação local o impede de cumprir com suas obrigações de acordo com estas BCR-P, incluindo qualquer um dos princípios de tratamento detalhados no artigo **Erreur ! Source du renvoi introuvable**. anterior e tenha um efeito substancial sobre as garantias aqui fornecidas, o referido membro das BCR deverá informar sem demora (i) ao(s) seu(s) cliente(s), (ii) à Webhelp SAS, (iii) ao membro das BCR da UE com responsabilidades delegadas em matéria de proteção de dados e (iv) ao DPO ou ao respectivo Líder Local de Privacidade/outra função de privacidade.

Quando um membro das BCR atuar como Encargado dos Dados, também se compromete a notificar sem demora a autoridade de proteção de dados

competente para seu cliente, se for o caso. Caso os pontos de contato relevantes dos membros das BCR tenham sido informados de acordo com o mecanismo de notificação mencionado anteriormente, a Webhelp SAS notificará o Órgão de Vigilância competente do EEE. Nesse caso, a Webhelp SAS se compromete a notificar esse requisito legal ao Órgão de Vigilância competente do EEE sem atrasos indevidos e, caso esse requisito legal exija a divulgação de Dados Pessoais pelo Membro das BCR em questão, a divulgar apenas os Dados Pessoais necessários em conformidade com a legislação local pertinente. Os membros das BCR especificarão a quais Titulares dos Dados esse requisito legal ou revelação pode afetar, qual autoridade solicita essa revelação e com base em qual fundamento legal. Em qualquer caso, os membros das BCR se comprometem a não transferir dados pessoais para autoridades públicas de forma massiva, indiscriminada e desproporcional.

Se um Membro das BCR tiver legalmente proibido realizar tal notificação, deverá fazer todo o possível para contornar essa proibição de acordo com a legislação local aplicável. A Webhelp SAS e esse Membro das BCR farão todo o possível para contornar a proibição a fim de notificar o Cliente e as Autoridades de Supervisão do EEE pertinentes. Para demonstrar seu melhor esforço para contornar a proibição, os Membros das BCR documentarão as medidas adotadas para tal fim e as colocarão à disposição do Órgão de Vigilância do EEE pertinente. Quando não for possível contornar a proibição, a Webhelp SAS deverá fornecer anualmente informações gerais sobre os números de divulgação de Dados Pessoais às autoridades pertinentes (por exemplo, número de solicitações de divulgação, tipo de dados solicitados, o solicitante se possível, etc.).

Além disso, quando um Membro das BCR estiver sujeito à legislação nacional dos Estados-Membros da UE que adicione alguns requisitos ou modalidades que possam impactar o Tratamento realizado por um Membro das BCR em virtude dessas BCR-P, esse Membro das BCR informará sem demora à Webhelp SAS e documentará os requisitos complementares aplicáveis de acordo com essa legislação nacional. Quando essa legislação nacional impor um nível de proteção mais alto aos Dados Pessoais, essa legislação nacional prevalecerá sobre as BCR-P..

Quando um membro das BCR localizado fora do EEE tiver motivos para acreditar que está ou esteve sujeito a leis ou práticas que não se ajustam à avaliação mencionada anteriormente, deverá notificar imediatamente o cliente ou o membro das BCR da UE que atua como Controlador de Dados em nome desse Cliente, que encaminhará a notificação ao Cliente. Após a notificação, o Cliente e/ou o Membro das BCR da UE que atua como Controlador de Dados deverão identificar prontamente as medidas apropriadas (por exemplo, medidas técnicas ou organizacionais para garantir a segurança e a confidencialidade) que deverão ser adotadas para lidar com a situação. Se não puderem garantir as salvaguardas adequadas para essa Transferência, esta deverá ser suspensa. Nesse caso, o Cliente e/ou o Membro das BCR da UE terão o direito de rescindir o contrato, se isso afetar o tratamento de dados pessoais de acordo com as BCR-P. Se o contrato envolver mais de duas partes, o Cliente e/ou o Membro das BCR da UE poderão exercer esse direito de rescisão apenas em relação ao Membro das BCR pertinente que não puder garantir um nível adequado de proteção de dados pessoais, salvo se as partes tiverem acordado de outra forma.

20.4 Dever de Cooperar

Em qualquer caso, os membros das BCR se comprometem a cooperar com as Autoridades de Supervisão do EEE, incluindo a aceitação de serem auditados ou inspecionados (nas instalações ou remotamente) por tais Autoridades de Supervisão, a considerar o aconselhamento e a acatar a decisão do Órgão de Vigilância do EEE competente que possa ser fornecida em relação a estas BCR-P. Os membros das BCR reconhecem e aceitam que os poderes e direitos de auditoria do Órgão de Vigilância competente não podem ser limitados, especialmente no que diz respeito à auditoria prática realizada por tal Órgão de Vigilância.

Quando atuarem como Controladores de Dados, os membros das BCR se comprometem a cooperar em um prazo razoável e na medida do razoavelmente possível com seus Clientes e a ajudá-los a cumprir a Legislação Aplicável sobre Proteção de Dados. Os membros das BCR também se assegurarão de que qualquer subprocessador que utilizem para processar dados pessoais esteja obrigado a cumprir o mesmo dever de cooperar e ajudar os membros das BCR e, quando necessário, o Controlador de Dados.

Os membros das BCR e, quando aplicável, seus respectivos representantes disponibilizarão ao Órgão de Vigilância do EEE, mediante solicitação, qualquer informação sobre as operações de tratamento cobertas pelas BCR-P, como os registros das atividades de tratamento.

Qualquer disputa relacionada com o exercício da supervisão do cumprimento das BCR-P por parte do Órgão de Vigilância competente será resolvida pelos tribunais do Estado Membro do referido Órgão de Vigilância, de acordo com a legislação processual desse Estado Membro. Os membros das BCR aceitam se submeter à jurisdição desses tribunais.

21. Programa de auditoria que alcance as BCR

Cada membro das BCR que atue como Operador será responsável pelo cumprimento das BCR-P e estará em condições de demonstrá-lo. Para esse fim, além dos requisitos estabelecidos no artigo 4.4 (Registro de atividades de tratamento) e no artigo 4.5 (Segurança), os membros das BCR devem cumprir o seguinte requisito relativo ao programa de auditoria de proteção de dados.

O membro das BCR se compromete a desenvolver e integrar em seu programa de auditoria a revisão de seu cumprimento com estas BCR-P. O programa de auditoria permitirá definir.:

- uma frequência razoável com a qual as auditorias serão realizadas;
- o escopo previsto da auditoria; e
- a equipe responsável pela auditoria.

O procedimento de auditoria está detalhado no **Apêndice 7 - Procedimentos para as Auditorias de Privacidade de Dados**. A auditoria abrange todos os aspectos destas BCR-P (por exemplo, aplicativos, sistemas de TI, bases de dados que processam dados pessoais, ou transferências subsequentes, decisões tomadas em relação aos requisitos obrigatórios em virtude de leis nacionais que entrem em conflito com as BCR-P, a revisão das condições contratuais utilizadas para transferências fora do Grupo aos Operadores de Dados, medidas corretivas, etc.),

incluindo os métodos e planos de ação que garantam a implementação das medidas corretivas. No entanto, não é necessário que tal programa de auditoria monitore todos os aspectos das BCR-P sempre que um membro das BCR for auditado, desde que todos os aspectos das BCR-P sejam supervisionados em intervalos regulares adequados para esse Membro das BCR.

Os membros das BCR se comprometem a realizar auditorias de forma periódica (pelo menos uma vez ao ano e/ou se houver indícios de descumprimento) para garantir a verificação do cumprimento das BCR-P ou considerando o nível de risco de uma atividade de Tratamento coberta por estas BCR-P para os direitos e liberdades dos Titulares dos Dados.

Além das auditorias periódicas, o DPO e/ou o membro pertinente da rede de privacidade (por exemplo, o Líder Local de Privacidade), ou qualquer outra função competente do grupo Concentrix, como o departamento de auditoria interna, poderão solicitar auditorias específicas (auditorias ad hoc). Essas auditorias poderão ser realizadas por auditores internos e/ou externos acreditados, assessorados pelo DPO e/ou pelo membro pertinente da rede de privacidade. O roteiro será iniciado e determinado pelo DPO e/ou pelo membro pertinente da rede de privacidade, conforme especificado no apêndice 7. Em qualquer caso, os auditores externos serão independentes e estarão sujeitos a uma obrigação de confidencialidade e/ou a uma obrigação legal de confidencialidade adequada.

O DPO é responsável por determinar o escopo das auditorias que devem ser realizadas. Para isso, ele pode consultar o Comitê de Privacidade e/ou encarregar a equipe de auditoria interna da Concentrix de determinar o escopo dessa auditoria. A auditoria poderá ser realizada pelo DPO do grupo e/ou pelos membros pertinentes da rede de privacidade (por exemplo, o Líder Local de Privacidade) e/ou pela equipe de auditoria interna do grupo Concentrix ou por qualquer outra função pertinente dentro da Concentrix, desde que:

- Seja garantida a independência dos responsáveis no exercício de suas funções para essas auditorias; e
- As pessoas encarregadas de auditar o cumprimento das BCR-P sejam substituídas, caso tal situação gere um conflito de interesses.

Os resultados de cada auditoria serão apresentados ao DPO do Grupo e/ou aos membros pertinentes da rede de privacidade (por exemplo, os Líderes Locais de Privacidade) e/ou ao Comitê de Privacidade e/ou aos membros da diretoria da Webhelp SAS para sua informação. O relatório final, a identificação de falhas e as medidas corretivas serão compartilhados e aplicados pelo Líder Local de Privacidade. Com base na avaliação do Líder Local de Privacidade, o relatório também poderá ser compartilhado, quando apropriado, com qualquer Referente de Privacidade do Negócio, com o gerente local de segurança, com os responsáveis pelo processo/sistema, com a diretoria matriz do grupo Concentrix ou com a diretoria do membro das BCR pertinente sujeito à auditoria, ou com qualquer outro funcionário interno necessário. Medidas corretivas serão definidas com uma ordem de prioridades para estabelecer um cronograma para a implementação dessas medidas.

A Concentrix reconhece que os Órgãos de Supervisão competentes do EEE, assim como os Clientes dos Membros das BCR, caso sejam diretamente afetados pela auditoria, podem solicitar a comunicação dos resultados da auditoria e, portanto, compromete-se a conceder-lhes acesso aos mesmos se assim solicitado. Os

resultados dos relatórios de auditoria e os relatórios de auditoria interna relevantes serão mantidos de forma que os Órgãos de Supervisão situados no EEE possam acessá-los, caso exerçam seu direito de auditoria, conforme estabelecido adiante. Além disso, os membros das BCR que atuem como Operadores ou Suboperadores de Dados se comprometem a apresentar, a pedido do Controlador dos Dados, suas instalações de tratamento de dados para auditoria das atividades de tratamento relativas ao Controlador dos Dados.

Os membros das BCR se comprometem a garantir que os Órgãos de Supervisão Competentes possam ter acesso aos resultados da auditoria, mediante solicitação, e não limitarão tais direitos, especialmente por motivos de confidencialidade, por exemplo, em relação à proteção de segredos comerciais.

Vale lembrar que o Membro das BCR autorizará qualquer Órgão de Supervisão competente do EEE a realizar auditorias de proteção de dados sobre qualquer questão relacionada às BCR-P. A esse respeito, cada membro das BCR permitirá ao Órgão de Supervisão do EEE auditar o membro das BCR pertinente para que o Órgão de Supervisão do EEE possa obter as informações necessárias para demonstrar o cumprimento dessas BCR-P pelo membro ou membros das BCR (veja também o artigo 13.4 anterior).

Além disso, quando um Membro das BCR atuar como Operador de Dados, seus Clientes poderão solicitar, com aviso prévio e com uma periodicidade razoável, e em qualquer caso, não mais de uma vez por ano, e às suas próprias custas, que a Concentrix realize auditorias para avaliar seu cumprimento ou o cumprimento de seus suboperadores com o Contrato de Serviços e/ou o Contrato de Tratamento de Dados, assim como com estas BCR-P.

"Nesse caso, o Membro das BCR deverá disponibilizar ao Cliente todas as informações necessárias para demonstrar o cumprimento da Legislação Aplicável sobre Proteção de Dados, dessas BCR-P e do Acordo de Tratamento de Dados aplicável, e permitir e colaborar com as auditorias, incluindo as inspeções, realizadas pelo Cliente ou por outro auditor designado pelo Cliente de acordo com o Acordo de Serviço.

Essa Auditoria cumprirá com o procedimento estabelecido no Apêndice 07.

22. Alterações às BCR-P

O DPO da Concentrix, com o apoio dos Líderes Locais de Privacidade, se certificarão de que as presentes BCR-P sejam mantidas atualizadas (por exemplo, levando em consideração as modificações no ambiente regulatório, as recomendações das autoridades de proteção de dados da UE, ou as mudanças no escopo das BCR-P).

Particularmente, o DPO manterá atualizada uma lista de entidades vinculadas pelas BCR-P. Quando uma nova entidade da Concentrix ficar efetivamente vinculada pelas BCR-P (como especificado no artigo 3.2), o DPO atualizará a lista e informará sem demora indevida todos os membros das BCR e os Órgãos de Supervisão pertinentes do EEE através do Órgão de Supervisão competente do EEE. Essa informação atualizada será disponibilizada aos Titulares dos Dados juntamente com as BCR-P e pelos mesmos meios.

Pelo menos uma vez ao ano, ou quando o DPO considerar necessário, a Webhelp SAS notificará essas mudanças aos Órgãos de Supervisão competentes do EEE. A

notificação dessas mudanças aos Órgãos de Supervisão do EEE será feita pelo menos uma vez ao ano através do Órgão de Supervisão do EEE competente, com uma breve explicação dos motivos que justificam a atualização. Os Órgãos de Supervisão também devem ser notificados uma vez ao ano, seguindo o mesmo processo, nos casos em que não houver mudanças.

A atualização ou notificação anual também deve incluir a renovação da confirmação de que a Webhelp SAS, como Membro Responsável das BCR, tomou as medidas apropriadas para garantir o pagamento de uma indenização por qualquer dano resultante de uma violação das BCR-P por parte dos Membros das BCR fora do EEE.

Da mesma forma, quando uma emenda tiver um impacto substancial nas BCR-P ou no nível de proteção dos direitos concedidos por essas BCR-P, a Webhelp SAS, com a assistência do DPO, compromete-se a informar sem demora os Membros das BCR e os Órgãos de Supervisão do EEE.

23. Descumprimento das BCR-P

Ao se tornar membro das BCR, o Exportador e o Importador dos Dados deverão cumprir com os seguintes requisitos:

- Nenhuma transferência será realizada para um membro das BCR a menos que o membro das BCR esteja efetivamente vinculado pelas BCR-P e possa cumpri-las.

- O Importador de Dados deverá informar sem demora ao Exportador de Dados se não puder cumprir as BCR-P, por qualquer motivo, incluindo as situações descritas com mais detalhes no artigo 13.3 das BCR-P..
- Se o Importador de Dados descumprir as BCR-P ou não puder cumpri-las, o Exportador de Dados ou o Cliente deverão suspender a Transferência.

O Importador de Dados deverá, a critério do Exportador de Dados, devolver ou apagar imediatamente os Dados Pessoais que tenham sido transferidos em virtude das BCR-P na totalidade, quando:

- O Exportador de Dados tenha suspendido a transferência e o cumprimento dessas BCR-P não seja restabelecido em um prazo razoável e, em qualquer caso, no prazo de um mês a partir da suspensão; ou

- O Importador de Dados descumpra de forma substancial ou persistente as BCR-P; ou
- O Importador de Dados descumpra uma decisão vinculante de um tribunal competente ou de um Órgão de Supervisão competente em relação às suas obrigações sob as BCR-P.

Os mesmos compromissos deverão ser aplicados a qualquer cópia dos dados. O Importador de Dados deverá certificar a eliminação dos dados ao Exportador de Dados.

Até que os dados sejam eliminados ou devolvidos, o Importador de Dados deverá continuar garantindo o cumprimento das BCR-P.

Se a legislação local aplicável ao Importador de Dados proibir a devolução ou eliminação dos dados pessoais transferidos, o Importador de Dados deverá garantir

que continuará assegurando o cumprimento das BCR-P e que tratará os dados apenas na medida e pelo tempo exigido por essa legislação local.

Para os casos em que as leis e/ou práticas locais aplicáveis afetem o cumprimento das BCR-P, veja o artigo 13.3 das BCR-P mencionado anteriormente. Se a legislação local aplicável ao Importador de Dados proibir a devolução ou eliminação dos dados pessoais transferidos, o Importador de Dados deverá garantir que continuará assegurando o cumprimento das BCR-P e que tratará os dados apenas na medida e pelo tempo exigido por essa legislação local.

Para os casos em que as leis e/ou práticas locais aplicáveis afetem o cumprimento das BCR-P, veja o artigo 13.3 das BCR-P mencionado anteriormente.

24. Terminação

Um membro das BCR que atue como Importador de Dados e que deixe de estar vinculado pelas BCR-P poderá conservar, devolver ou eliminar os dados pessoais recebidos em virtude das BCR-P.

Se o Exportador de Dados e o Importador de Dados concordarem que os dados podem ser conservados pelo Importador de Dados, a proteção deve ser mantida de acordo com o Capítulo V do GDPR e como refletido no Artigo 6 das BCR-P.

25. Apêndices

- Apêndice 01 - Lista de Membros das BCR vinculados pelas BCR-C e os e-mails de contato de privacidade local
- Apêndice 02 - Definições para as BCR e procedimentos
- Apêndice 03 - Governança e organização da Privacidade
- Apêndice 04 - Programa de treinamento e conscientização.
- Apêndice 05 - Procedimento para solicitações dos Titulares dos Dados onde a Concentrix atua como Controlador dos Dados.
- Apêndice 06 - Procedimento para solicitações dos Titulares dos Dados onde a Concentrix atua como Operador dos Dados.
- Apêndice 07 – Procedimento de Auditoria
- Apêndice 08 - Procedimento em caso de Violação de Dados Pessoais
- Apêndice 09 – Avaliação de Impacto na Proteção de Dados
- Apêndice 10 – Política de Segurança da Informação
- Apêndice 11-A - Lista BCR-C de propósitos do processamento e categorias relacionadas com os Dados Pessoais e os Titulares dos Dados. (Escopo Material)
- Apêndice 11-B - Lista BCR-P de propósitos do processamento e categorias relacionadas com os Dados Pessoais e os Titulares dos Dados. (Escopo Material)

CONTROLE DE DOCUMENTO

Versão	Atualização	Resumo das modificações
0.1	27/02/2022	Aprovação final
0.2	01/01/2023	Atualização da lista de Membros das BCR
0.3	24/02/2023	Atualização da lista de Membros das BCR
0.4	01/04/2024	Re branding y formato Ajuste às recomendações do EDPB 1/2022, revogando e substituindo o WP56_Rev01

Frequência de Revisão	Este documento será revisado pelo menos uma vez por ano ou sempre que houver mudanças nas entidades da Webhelp.
Data de Emissão	25/05/2018
Domínio	Privacidade
Classificação	Público
Referência	EN__GPPriv-01-Normas Corporativas Vinculantes - Controlador

Anexo 01

Lista de entidades da Concentrix sujeitas às BCR e contatos de e-mail de privacidade locais

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
1.	Webhelp Albania Shpk	Rruga Dervish Hima, Stadiumi Air Albania, Qendra e Biznesit, Shkalla BC, nr.BC, Niveli +3, 1019 Tirana	Albânia	privacy@it.webhelp.com
2.	Webhelp Algerie SPA	16bis, ciudad Bois des Cars 2 16047 Dely Ibrahim	Argélia	privacy@dz.webhelp.com
3.	Webhelp Australia Pty Ltd	Level 16, 201 Elizabeth Street Sydney NSW 2000	Australia	privacy@my.webhelp.com
4.	Webhelp Austria GmbH	Floridsdorfer Haptstrasse 1, 1210 Vienna	Austria	privacy@de.webhelp.com
5.	Webhelp Payment Services Benelux, SA	Avenue Louise, 87 - 1050 Bruxelles	Bélgica	privacy@wps.webhelp.com
6.	Webhelp Benín	Immeuble le Jatoba, avenue Jean-Paul II, lot 20, zone résidentielle portuaire; (Nouveau site en cours : Parcelle F G Ilot 40002,quartier Enagnon Akpakpa Cotonou)	Benín	Privacy@fr.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
7.	Webhelp BH d.o.o. Sarajevo	Josipa Stadlera 6, 71000, Sarajevo	Bosnia-Herzegovina	privacy@de.webhelp.com
8.	Services Tech Experience Inovaçao e technologia em relacionamento Ltda	Rua Marechal Deodoro, 314 6th Floor, Sets 601-606, Centro Curitiba, Paraná, 80.010-010	Brasil	protecciondedatos@onelinkbpo.com
9.	Services Assessoria Digital Ltda	Rua Marechal Deodoro 314, 11th floor,Centro Curitiba, Paraná, 80.010-010	Brasil	protecciondedatos@onelinkbpo.com
10.	Webhelp Bulgaria EOOD	Blvd. Totleben, Business-Center Sofia City-West 53-55, 1606, Sofia	Bulgária	privacy@de.webhelp.com
11.	Les services Webhelp, Inc	880 Rue Roy Est, QC H2L 1E6, Montreal, Quebec	Canadá	protecciondedatos@onelinkbpo.com
12.	Webhelp Business Consulting (Shanghai) Co. Ltd	Room 368, Unit 302, No. 211, North Fude Road, Shanghai FTZ	China	privacy@my.webhelp.com
13.	Webhelp (Suzhou) Data Services Co. Ltd	Unit 2605B, 26th Floor, West Tower, China Overseas Fortune Center, No. 9 Suzhou Avenue West, Suzhou Industrial Park	China	privacy@my.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
14.	Onelink SAS	Carrera 52 No. 65 91 DE 740 CENTRO COMERCIAL AVENTUR, Medellín	Colômbia	protecciondedatos@onelinkbpo.com
15.	Onelink International SAS	Avenida carrera 19 # 28 80 Cc Empresarial Calima Of 401, Bogotá	Colômbia	protecciondedatos@onelinkbpo.com
16.	Experts Colombia SAS	Carrera 52 No. 65 61, Medellín	Colômbia	protecciondedatos@onelinkbpo.com
17.	GetcomColombia SAS	Diagonal 55 nº 37 41 OF. 601	Colômbia	protecciondedatos@onelinkbpo.com
18.	Getcom Servicios SAS	Diagonal 55 Av 37 41 OF 701, Bello	Colômbia	protecciondedatos@onelinkbpo.com
19.	Webhelp Enterprise Sales Solutions, s.r.o	Vaclavské náměstí 808/66, 11000 Praga, Nové Mesto	República Checa	privay@cz.webhelp.com
20.	Webhelp Denmark, AS	Borgmester Christiansens Gade 50, 2, 2500, Copenhague	Dinamarca	privacy@nordic.webhelp.com
21.	Webhelp Egypt	plot No. 53, First District, City Center New Cairo, Cairo	Egipto	privacy@eg.webhelp.com
22.	Onelink SA de CV	Avenida Albert Einstein y Bulevar, San Salvador.	El Salvador	protecciondedatos@onelinkbpo.com
23.	Tetel SA de CV	Avenida Albert Einstein y Bulevar, San Salvador.	El Salvador	protecciondedatos@onelinkbpo.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
24.	Getcom International SA de CV	Boulevard Los Próceres, Colonia Palermo Edificio Ex Panades, No. 350, Frente a UCA, San Salvador, San Salvador.	El Salvador	protecciondedatos@onelinkbpo.com
25.	RH-T SA de CV	Avenida Albert Einstein y Bulevar, San Salvador.	El Salvador	protecciondedatos@onelinkbpo.com
26.	Webhelp OÜ	Tartu mnt 63, Tallin 10115	Estônia	privacy@nordic.webhelp.com
27.	Webhelp Finland, Oy	Palkkatilanportti 1 FI-0240 Helsinki	Finlândia	privacy@nordic.webhelp.com
28.	GoBeyond Partners, SAS	3/5 rue d'Héliopolis y 17/19 rue Guillaume Tell , 75017 París	França	Privacy@fr.webhelp.com
29.	Webhelp, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	França	Privacy@fr.webhelp.com
30.	Webhelp Conseil, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	França	Privacy@fr.webhelp.com
31.	W Automobile Services, SAS	3/5 rue d'Héliopolis y 17/19 rue Guillaume Tell	França	Privacy@fr.webhelp.com
32.	Webhelp France, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	França	Privacy@fr.webhelp.com
33.	Webhelp Caen, SAS	1 rue Jean Perrin, 14460 Colombelles	França	Privacy@fr.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
34.	Webhelp Compiègne, SAS	ZAC du Parc Tertiaire - 98 impasse Les Terres auprès des Iles, 60610, Compiègne	França	Privacy@fr.webhelp.com
35.	Webhelp Fontenay, SAS	6 Rue de l'Innovation, 85200 Fontenay-le-Comte	França	Privacy@fr.webhelp.com
36.	Marnix French ParentCO, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	França	privacy@webhelp.com
37.	Marnix French TOPCO, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	França	privacy@webhelp.com
38.	Marnix, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	França	privacy@webhelp.com
39.	WowHoldCo, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	França	privacy@webhelp.com
40.	Webhelp Gray, SAS	ZAC GRIS SUD 70100 GRAY	França	privacy@fr.webhelp.com
41.	Webhelp Montceau, SAS	16 rue Saint-Eloi, 71300, Montceau les Mines	França	privacy@fr.webhelp.com
42.	Webhelp Vitré, SAS	Parque de Actividad Etrelles, 35370 Etrelles	França	privacy@fr.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
43.	Webhelp University France, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	França	privacy@fr.webhelp.com
44.	Webhelp Prestations, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	França	privacy@fr.webhelp.com
45.	Webhelp WTG, SAS	39 rue des métissages 59200 Tourcoing	França	privacy@fr.webhelp.com
46.	Webhelp Medica Customer Expérience	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	França	privacy@webhelpmedica.com ; privacy@patientys.webhelp.com
47.	Patientys, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	França	privacy@webhelpmedica.com ; privacy@patientys.webhelp.com
48.	MED-TO-MED, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	França	privacy@webhelpmedica.com ; privacy@patientys.webhelp.com
49.	WGE (Webhelp Grand-Est, SAS)	Technopole, 9 rue Thomas Edison, Metz	França	privacy@fr.webhelp.com
50.	Webhelp Médica, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	França	privacy@webhelpmedica.com ; privacy@patientys.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
51.	Webhelp SFIA, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	França	privacy@fr.webhelp.com
52.	Webhelp WCS, SAS	12 Rue Alfred Kastler 71530 Fragnes-La Loyère	França	privacy@fr.webhelp.com
53.	Netino, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	França	privacy@fr.webhelp.com
54.	Solvencia, S.A.S.	450 Rue Félix Esclangon, 73290 La Motte-Servolex	França	privacy@wps.webhelp.com
55.	Webhelp O2C Holding, SAS	450 Rue Félix Esclangon, 73290 La Motte-Servolex	França	privacy@wps.webhelp.com
56.	Webhelp KYC Servicios, SAS	450 Rue Félix Esclangon, 73290 La Motte-Servolex	França	privacy@wps.webhelp.com
57.	Webhelp Payment Services France, SAS	450 Rue Félix Esclangon, 73290 La Motte-Servolex	França	privacy@wps.webhelp.com
58.	Webhelp Payment Services Deutschland, GmbH	Frankfurter Str. 151A, 63303 Dreieich	Alemanha	privacy@wps.webhelp.com
59.	Webhelp Sun Holding GmbH	Tullnaustrasse 20, 90402, Nuremberg	Alemanha	privacy@de.webhelp.com
60.	Webhelp Holding Germany GmbH	Tullnaustrasse 20, 90402 Nuremberg	Alemanha	privacy@de.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
61.	Webhelp Deutschland GmbH	Tullnaustrasse 20, 90402 Nuremberg	Alemanha	privacy@de.webhelp.com
62.	RIGHTHEAD GmbH	Tullnaustrasse 20, 90402 Nuremberg	Alemanha	privacy@de.webhelp.com
63.	Webhelp Ghana Ltd	SU TOWER, N°18, Castle Road, North Ridge, Accra	Ghana	privacy@fr.webhelp.com
64.	Webhelp Hellas Business Enterprise Sales SMLTD (MEPE en griego)	36 Voukourestiou Str 10673 Atenas	Grécia	privacy@gr.webhelp.com
65.	Onelink Guatemala S.A.	15 Avenida 17-30 Zona 13, Oficina 201, Guatemala, Guatemala	Guatemala	protecciondedatos@onelinkbpo.com
66.	Onelink Soluciones Guatemala SA	15 Avenida 17-40 zona 13, Torre 1, Nivel 1 Edificio Tetra Center, Ciudad de Guatemala	Guatemala	protecciondedatos@onelinkbpo.com
67.	Inversiones Xperts Guatemala SA	15 Avenida 17-40 zona 13, Torre 1, Nivel 1 Edificio Tetra Center, Ciudad de Guatemala	Guatemala	protecciondedatos@onelinkbpo.com
68.	Gobeyond Partners Asia Limited	31/F Tower Two Times Square 1, Matheson St., Causeway Bay, Hong Kong	Hong Kong	privacy@my.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
69.	Webhelp India Private Ltd	Escritório corporativo : Plata Baja, Torre A, SP Infocity, Udyog Vihar, Phase-1, Gurugram-122001, Haryana , India	India	privacy@uk.webhelp.com
70.	SELLBYTEL Marketing Services India Private Ltd	Escritório corporativo : - Planta baja, Torre A, SP Infocity, Udyog Vihar, Fase-1, Gurugram-122001, Haryana, India	India	privacy@uk.webhelp.com
71.	Webhelp Israel Ltd.	Yigal Alon 94, torre Alon 1 Tel Aviv, Tel Aviv	Israel	privacy@tr.webhelp.com
72.	Webhelp Payment Services Italia, SRL	Via Gozzano Guido 14 - 20092 Cinisello Balsamo	Itália	privacy@wps.webhelp.com
73.	Webhelp Payment Services France succursale Italie	Via Maurizio Gonzaga n° 7	Itália	privacy@wps.webhelp.com
74.	Webhelp Enterprise Sales Solutions Italy	Via Torri Bianche, 7, 20871 Vimercate MB, Italy	Itália	privacy@it.webhelp.com
75.	Webhelp Cote d'Ivoire	Immeuble PIA, Avenue Abdoulay Fadiga, Plateau Abidjan - 01 BP 7171 ABJ 01	Costa do Marfim	privacy@ci.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
76.	WH Abidjan Le Workshop	Indenie, 6 rue des Sambas 01 BP 743 ABJ 01, Plateau Abidjan - 01 BP 743 ABJ 01	Costa do Marfim	privacy@ci.webhelp.com
77.	Webhelp SAS (succursale Côte d'Ivoire)	Immeuble PIA, Avenue Abdoulay Fadiga, Plateau Abidjan - 01 BP 7171 ABJ 01	Costa do Marfim	privacy@ci.webhelp.com
78.	Webhelp Japan KK	Tokyo Club Building 11F, 3-2-6 Kasumigaseki, Chiyoda-ku, Tokyo	Japão	privacy@my.webhelp.com
79.	Webhelp Jordan LLC	Rafiq Al Hariri Ave 1, Ammán	Jordânia	privacy@jo.webhelp.com
80.	IQ-to-Link shpk	Rr. Ukshin Hoti nr. 121	Kosovo	privacy@de.webhelp.com
81.	Webhelp Kosovo LLC	Rr. Ukshin Hoti nr. 120, 10000, Pristina	Kosovo	privacy@de.webhelp.com
82.	Webhelp Latvia SIA	Krišjāņa Valdemāra iela 21-18	Letônia	privacy@jo.webhelp.com
83.	Webhelp SIA	Skanstes iela 54A	Letônia	privacy@de.webhelp.com
84.	Webhelp Madagascar, SA (zone franche)	Bâtiment TITAN 2, Zona Galaxy Andraharo, Antananarivo 101	Madagascar	privacy@mg.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
85.	Netino Madagascar	Lot II M92 Antsakaviro - Ambodirotra Cua Antananarivo 101 Analamanga	Madagascar	privacy@mg.webhelp.com
86.	Webhelp Malasia Sdn Bhd	Menara Exchange 106, Level 6, Lingkaran TRX, Jalan Tun Razak, 55188 Kuala Lumpur, Malaysia	Malásia	privacy@my.webhelp.com
87.	Onelink México SA de CV	BOULEVARD 300 ENTRE CALLE CDA MEZTISOS - VILLAS DEL REY - CAJEME-OBREGÓN SONORA-MÉXICO, 85136, Ciudad Obregón	México	protecciondedatos@onelinkbpo.com
88.	Onelink Servicios SA de CV	BOULEVARD 300 ENTRE CALLE CDA MEZTISOS - VILLAS DEL REY - CAJEME-OBREGÓN SONORA-MÉXICO, 85136, Ciudad Obregón	México	protecciondedatos@onelinkbpo.com
89.	Webhelp Marruecos, SA	43 av Ibn Sina-Agdal-Rabat	Marrocos	privacy@ma.webhelp.com
90.	Webhelp SAS Succursale	28 Avenue Allal Ben Abdellah - (Dirección comercial: 43 av Ibn Sina-Agdal-Rabat)	Marrocos	privacy@ma.webhelp.com
91.	Webhelp Services, SA	15, Avenue Annakhil (Dirección comercial: 43	Marrocos	privacy@ma.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
		av Ibn Sina-Agdal-Rabat)		
92.	Webhelp Contact Center, S.A.	N°50 BLOQUE F 11 IMMEUBLE AL FIDIAN I ET IMMEUBLE AL FIDIAN II AVENIDA HASSAN I CITE DAKHLA (Endereço comercial: 43 av Ibn Sina-Agdal-Rabat)	Marrocos	privacy@ma.webhelp.com
93.	Webhelp Multimedia, SA	6, rue Lalla Nezha, 30000 Fès	Marrocos	privacy@ma.webhelp.com
94.	Webhelp GRC, SA	43 Avenida Ibn Sina, 10000 Rabat	Marrocos	privacy@ma.webhelp.com
95.	Webhelp Tecnopolis, SA	Agdal, 25, Rue Oued Al Makhazine (Endereço comercial l: 43 av Ibn Sina-Agdal-Rabat)	Marrocos	privacy@ma.webhelp.com
96.	Webhelp University Maroc, SARL	15 av Annakhil, (Endereço comercial : 43 av Ibn Sina-Agdal-Rabat)	Marrocos	privacy@ma.webhelp.com
97.	Webhelp Agadir, SA	Quartier Industriel, Avenue Hassan II, Immeuble Jaouhara (Endereço comercial: 43	Marrocos	privacy@ma.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
		av Ibn Sina-Agdal-Rabat)		
98.	Webhelp Fès, SA	112 Avenue des FAR Champs de Course ville nouvelle (Endereço comercial : 43 av Ibn Sina-Agdal-Rabat)	Marrocos	privacy@ma.webhelp.com
99.	Webhelp Meknès, SA	Immeuble Angle Rue Badir Al Kobra et Rue Sebou angle rue Badr al Korba, Meknes (Endereço comercial : 43 av Ibn Sina-Agdal-Rabat)	Marrocos	privacy@ma.webhelp.com
100.	Webhelp Marrakech, SA	Quartier Industriel, Avenue Hassan II, Immeuble Jaouhara (Endereço comercial : 43 av Ibn Sina-Agdal-Rabat)	Marrocos	privacy@ma.webhelp.com
101.	Webhelp Afrique	CFC Bridge, lot 58, Rez de Chaussée (Core 1), quartier Casa-Anfa, Hay Hassani - Casablanca	Marrocos	privacy@ma.webhelp.com
102.	Webhelp Netherlands Holding, BV	Amersfoortsestraat 28, 3821CB, Amersfoort	Países Baixos	privacy@nl.webhelp.com
103.	Customer Contact Management Group, BV	Amersfoortsestraat 28, 3821CB, Amersfoort	Países Baixos	privacy@nl.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
104.	Webhelp Nederland, BV	Koraalrood 50, 2718SC Zoetermeer	Países Baixos	privacy@nl.webhelp.com
105.	Webhelp Enterprise BV	Brammelerstraat 8, 7511JG Enschede	Países Baixos	privacy@nl.webhelp.com
106.	Stacelet Holding, BV	Colosseum 42, 7521 PT Enschede	Países Baixos	privacy@nl.webhelp.com
107.	Telecats BV	Colosseum 42, 7521 PT Enschede	Países Baixos	privacy@nl.webhelp.com
108.	Customer Contact Performance Group B.V.	Herengracht 501 H, 1017B, Amsterdam	Países Baixos	privacy@nl.webhelp.com
109.	CCPG Ámsterdam BV	Herengracht 501 H, 1017B, Amsterdam	Países Baixos	privacy@nl.webhelp.com
110.	CCPG Utrecht BV	Herengracht 501 H, 1017B, Amsterdam	Países Bajos	privacy@nl.webhelp.com
111.	Xpertos Nicaragua SA	Plaza El Sol 2 C. Sur, 1C. Este, Casa No. 26, Los Robles Managua	Nicarágua	protecciondedatos@onelinkbpo.com
112.	Onelink Nicaragua S.A.	Barrio Largaespada. B. Largaespada Busto Jose Marti 3 C al Este 1 C al Norte, Managua	Nicarágua	protecciondedatos@onelinkbpo.com
113.	Webhelp Company Severna Makedonija DOOEL Skopje	Bul. VMRO 1, 1000, Skopje, North-Macedonia	Macédoine do Norte	privacy@de.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
114.	Webhelp Norway, AS	Storgata 38, 0182 Oslo	Noruega	privacy@nordic.webhelp.com
115.	Webhelp Norway Consulting AS	Storgata 38, 0182 Oslo	Noruega	**privacy@nordic.webhelp.com**
116.	Webhelp Perú SAC	Calle Santa Inés Nro. 115, Urbanización Industrial Santa Rosa, distrito Ate, Lima	Perú	protecciondedatos@onelinkbpo.com
117.	BPO Consultoría SAC	Jirón Marcos Farfán, n° 3468, Lima	Perú	protecciondedatos@onelinkbpo.com
118.	Webhelp Philippines, Inc.	12th floor, Makati Sky Plaza, 7788 Ayala avenue, Makati City, 1223	Filipinas	privacy@my.webhelp.com
119.	Webhelp Poland Sp. z.o.o.	Ul. Taneczna 30, PL 02-829, Warszawa	Polônia	privacy@de.webhelp.com
120.	Webhelp Sun Portugal, Unipessoal, Lda	Avenida Professor Cavaco Silva, Tagus Park, Edificio Qualidade, bloco A-2, 2470-296 Porto Salvo, parish of Porto Salvo, Oeiras	Portugal	privacy@pt.webhelp.com
121.	Webhelp Oeiras, Lda	Avenida Professor Cavaco Silva, Tagus Park, Edificio Qualidade, bloco A-2, Lisboa	Portugal	privacy@pt.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
122.	Webhelp Lisboa, Unipessoal, Lda	Avenida D. João II, nº 43, Torre Fernão de Magalhães, 15º Piso, freguesia de Parque das Nações, 1998-025, Lisboa	Portugal	privacy@pt.webhelp.com
123.	Webhelp SAS Succursale em Portugal	Avenida D. João II, nº 43, Torre Fernão de Magalhães, 15º Piso, freguesia de Parque das Nações, 1998-025 Lisboa	Portugal	privacy@pt.webhelp.com
124.	Webhelp Norte, Unipessoal LDA	Av. Mediterrâneo 1, 1990-203 Lisboa, freguesia de Parque das Nações, LIsboa	Portugal	privacy@pt.webhelp.com
125.	Righthead - Empresa de Trabalho Lda	Avenida Professor Cavaco Silva, Tagus Park, Edificio Qualidade, bloco A-2	Portugal	privacy@pt.webhelp.com
126.	WH New Generation Lisbon	Av. Mediterrâneo 1, 1990-203 Lisboa, freguesia de Parque das Nações, 1998-025, Lisboa	Portugal	privacy@pt.webhelp.com
127.	Webhelp SFIA, Filial em Portugal	Av. Mediterrâneo 1, 1990-203 Lisboa, freguesia de Parque das Nações, 1998-025, Lisboa	Portugal	privacy@pt.webhelp.com
128.	Webhelp Payment Services España, Filial em Portugal	Av. Mediterrâneo 1, 1990-203 Lisboa, freguesia de Parque das Nações, 1998-025, Lisboa	Portugal	privacy@wps.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
129.	Webhelp Romania SRL	Sector 1, Str. Doctor Iacob Felix, nr. 63-69, et. 2	Romênia	privacy@ro.webhelp.com
130.	Pitech Plus SA	Strada Câmpul Pâinii nr.3-5, etajul 3	Romênia	privacy@ro.webhelp.com
131.	MindMagnet Plus SRL	Strada Câmpul Pâinii nr.3-5, etajul 3, 400058, Cluj-Napoca	Romênia	privacy@ro.webhelp.com
132.	Webhelp Senegal SAS	Almadies, Pointe des Almadies, en face King Fahd, fahd Palace, 284, TF n°284/NGA Dakar	Senegal	privacy@sn.webhelp.com
133.	Webhelp SAS Succursale Senegal	Almadies, Imm Serenity Pointe des Almadies, en face King Fahd, fahd Palace TF n°284/NGA Dakar	Senegal	privacy@sn.webhelp.com
134.	Webhelp d.o.o Beograd	Makedonská 30, III. Floor, 11000, Beograd	Servia	privacy@de.webhelp.com
135.	Webhelp Singapur Pte Ltd	9 Raffles Place, #26-01 Republic Plaza, Singapore 048619	Singapura	privacy@my.webhelp.com
136.	Webhelp Slovakia, s.r.o.	Staromestská 3 811 03, Bratislava - mestská časť Staré Mesto	República Eslovaca	privacy@it.webhelp.com
137.	Webhelp Holding Germany GmbH	City Centre - Republic square, 1000, Ljubljana	Eslovênia	privacy@de.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
	(sucursal en Eslovenia)			
138.	Concentrix South Africa (Pty) Pty Ltd	19 Ameshoff Street, Braamfontein, Johannesburg, 2001	África do Sul	privacy@uk.webhelp.com
139.	Webhelp SAS, Sucursal en España	Plaza Solymar s/n, Edificio Benalmar, 29630 Benalmádena, Málaga	Espanha	**privacy@es.webhelp.com**
140.	Direct Médica Ibérica SL	CL LAGASCA, 95, 28006 MADRID	Espanha	privacy@webhelpmedica.com
141.	Webhelp Malaga SLU	Plaza Solymar s/n Edificio WEBHELP, 29630 Benalmádena, Málaga	Espanha	privacy@es.webhelp.com
142.	Webhelp Payment Services Espana SA	Calle Vallespir, número 19, módulo 3, planta 1ª de Sant Cugat del Vallès	Espanha	privacy@wps.webhelp.fr
143.	Webhelp Spain Business Process Outsourcing S.L.	Avda. Diagonal 197 Barcelona, 08018	Espanha	privacy@es.webhelp.com
144.	Webhelp Spain Holding SLU	Av. Diagonal 97, 12 Barcelona 08018	Espanha	privacy@es.webhelp.com
145.	Telenamic NV	Zonnebloemstraat 50, Paramaribo	Suriname	privacy@sr.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
146.	Webhelp Sweden AB	Box 4006, 16904 Solna	Suécia	
147.	Webhelp IT Services AB	Box 4006, 16904 Solna	Suécia	privacy@nordic.webhelp.com
148.	Webhelp Schweiz AG	Richtisstraße 5, 8304 Wallisellen	Suíça	privacy@de.webhelp.com
149.	Webhelp (Thailand) Limited	87/1 Capital Tower All Seasons Place, Unit 1604-6 Floor 16, Pathumwan District, 10330, Bangkok	Tailândia	privacy@my.webhelp.com
150.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş. (Centro de Atendimento Webhelp e Sociedade Anônima de Atendimento ao Cliente).	Merkez Mh. Ayazma Cd. Papirus Plaza No.37/42	Turquia	privacy@tr.webhelp.com
151.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş. Bingöl Branch (Centro de Atendimento Webhelp e Sociedade Anônima de Atendimento ao Cliente).	Bingöl Üniversitesi Fen Edebiyat Fakültesi No:Merkezi Derslik Birimi Bodrum Kat:1 Merkez/Bingöl, 12000 Bingöl	Turquia	privacy@tr.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
152.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş.İzmir 2 Branch (Centro de Atendimento Webhelp e Sociedade Anônima de Atendimento ao Cliente).	Beyazevler Mahallesi Akçay Cad. No: 99/2, 35410 Gaziemir/ Izmir	Turquia	privacy@tr.webhelp.com
153.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş.Van 2 Branch (Centro de Atendimento Webhelp e Sociedade Anônima de Atendimento ao Cliente).	Vali Mithat Bey Mahallesi Cemaller Sk. Roza Aprt Sit. No: 9 A ipekyolu/65100 Van,	Turquia	privacy@tr.webhelp.com
154.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş.Ümraniye Branch (Centro de Llamadas Webhelp y Sociedad Anónima de Atención al Cliente).	Fatih Sultan Mehmet Mahallesi Balkan Cad. Casper Plaza İş Merkezi Apt. No: 47/1 Ümraniye / 34771 Istanbul	Turquia	privacy@tr.webhelp.com
155.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş.Bursa Branch (Centro de Chamadas Webhelp e Sociedade	Panayır Mahallesi 3. Pınar Cad. No: 345 B Osmangazi/ 16250 Bursa	Turquía	privacy@tr.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
	Anônima de Atendimento ao Cliente).			
156.	Bin Çağrı Hizmetleri A.Ş. (Sociedade Anônima de Serviços Bin Call)	Bingöl Üniversitesi Fen Edebiyat Fakültesi - Bingöl	Turquía	privacy@tr.webhelp.com
157.	Webhelp İnsan Kaynkaları Danışmanlık ve Destek Hizmetleri A.Ş. (Sociedade Anônima de Serviços de Suporte e Consultoria de Recursos Humanos Webhelp)	Merkez Mh. Ayazma Cd. Papirus Plaza No.37/42, 34406; Kağıthane - Istanbul	Turquía	privacy@tr.webhelp.com
158.	Teknofix Telekomünikasyon ve Bilişim Hizmetleri A.Ş. (Sociedade Anônima de Serviços de Informação e Telecomunicações Teknofix)	Aydınevler Mah. Aslanbey Cad. No:1 D:5-6, Küçükyalı, Maltepe, Estambul	Turquía	privacy@tr.webhelp.com
159.	Teknofix Telekomünikasyon ve Bilişim Hizmetleri A.Ş. Istanbul Kagithane Branch (Sociedade Anônima de Serviços de Informação e	Merkez Mh. Ayazma Cd. Papirus Plaza No.37/42, 3440 Kağıthane - Istanbul	Turquía	privacy@tr.webhelp.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
	Telecomunicações Teknofix)			
160.	Teknofix Telekomünikasyon ve Bilişim Hizmetleri A.Ş. Ankara Basinevleri Branch (Sociedade Anônima de Serviços de Informação e Telecomunicações Teknofix)	Basınevleri Mah. Yankılar Sok. No:16 Keçiören, Ankara	Turquía	privacy@tr.webhelp.com
161.	Telecom Service Centres Ltd	11 Central Park Avenue, Central Business Park, Larbert, Falkirk, FK5 4RX,	Reino Unido	privacy@uk.webhelp.com
162.	Webhelp Payment Services UK Ltd	C/o Civvals Limited, 50 Seymour Street, London W1H 7JG	Reino Unido	privacy@wps.webhelp.com
163.	Webhelp Medica UK Limited	Building 2, 1 Nunnery Square, S2 5DD, Sheffield	Reino Unido	privacy@webhelpmedica.com
164.	Webhelp USA Group Inc.	1111 Brickell Avenue, Suite 11, FL 33131, Miami	EE.UU.	protecciondedatos@onelinkbpo.com
165.	Webhelp USA LLC	1111 Brickell Avenue, Suite 11, FL 33131, Miami	EE.UU.	protecciondedatos@onelinkbpo.com
166.	Webhelp US LLC	1111 Brickell Avenue, Suite 11, FL 33131, Miami	EE.UU.	protecciondedatos@onelinkbpo.com

#	Entidade Concentrix (Membros das BCR)	Endereço postal	País	Endereço de e-mail para lembrete de privacidade: você também pode entrar em contato com o DPO do Grupo a qualquer momento em dpo@concentrix.com
167.	Webhelp Logbox USA	110 West 40th Street , Suite 1903 New York, NY 10018	EE.UU.	protecciondedatos@onelinkbpo.com
168.	Webhelp Americas LLC	80 SW 8TH ST, SUITE 2900, FL 33130, Miami	E.E.U.U.	protecciondedatos@onelinkbpo.com
169.	Webhelp California Inc.	200 Madison Avenue, Suite, 1901, NY 10016,New York	EE.UU.	protecciondedatos@onelinkbpo.com

CONTROLE DE DOCUMENTO

Versão	Data de atualização	Resumo das modificações
0,1	27/02/2022	Aprovação final
0,2	02/02/2023	Lista revisada com base na dissolução e novas entidades
0,3	04/01/2024	Rebranding e formato Atualizações dos membros das BCR (refletindo ex-membros das BCR liquidadas, novas entidades e mudanças de nomes)

Frequência de revisão	Este documento será revisado pelo menos uma vez por ano ou em caso de mudanças.
Data de publicação	25/05/2018
Domínio	Privacidade
Classificação	Público
Referência	Apêndice 1 das BCR - Lista de membros das BCR e contatos de privacidade locais

Anexo 2
Definições para as BCR e Procedimentos

“Legislação aplicável sobre proteção de dados”	Significa, na seguinte ordem de prevalência: (i) o Regulamento Europeu 2016/679 relativo ao Tratamento de Dados Pessoais a partir da sua data de aplicação (‘GDPR’), (ii) as leis e regulamentos nacionais dos Estados-membros da UE relativos ao Tratamento de Dados Pessoais e que implementam o GDPR e (iii) qualquer normativa relativa ao Tratamento de Dados Pessoais aplicável durante a vigência desta Política de Privacidade..
“Norma Corporativa Vinculante" ou BCR	Refere-se às políticas e procedimentos de proteção de Dados Pessoais aos quais os Membros das BCR aderem para transferências ou um conjunto de transferências de Dados Pessoais a um Controlador ou Processador de Dados em um ou mais países terceiros dentro do grupo Concentrix
“Membro das BCR”	Refere-se a qualquer filial do grupo Concentrix que tenha assinado e esteja obrigada pelas BCR-C e/ou pelas BCR-P e que, como tal, tenha se comprometido a cumprir essas BCR; os membros das BCR estão enumerados no Anexo 01 dessas BCR-C e BCR-P.
“Cliente corporativo”	Significa qualquer terceiro que contrate com a Concentrix e atue como controlador de dados, cujos dados pessoais sejam tratados por um membro das BCR que atue como Responsável pelos dados de acordo com suas instruções documentadas.
“AS Competente" ou "Autoridade de Supervisão Competente”	Autoridade de Controle do EEE para o exportador de dados
“Dados" ou "Informação”	Refere-se a qualquer tipo de informação acessível individualmente por meios eletrônicos ou de outro tipo, como registros, dados pessoais, documentos ou outros materiais.
“Base de dados”	É uma coleção de obras, dados, informações ou outros materiais independentes dispostos de forma sistemática ou metódica e acessíveis individualmente por meios eletrônicos ou de outro tipo.
"Exportador de dados "	Refere-se ao Controlador ou Processador de Dados que transfere os Dados Pessoais para um país terceiro não pertencente ao EEE

“Importador de dados”	Refere-se ao Controlador ou Processador de Dados que recebe os dados pessoais.
“Responsável pelos dados” ou “Responsável”	Significa a pessoa física ou jurídica, autoridade pública, agência ou outro organismo que, sozinho ou em conjunto com outros, determine os fins e os meios do Tratamento de Dados Pessoais.
“Encarregado pelo tratamento dos dados” o “Encarregado”	Significa uma pessoa física ou jurídica, autoridade pública, agência ou outro organismo que processa Dados Pessoais em nome do Controlador de Dados.
“Titular dos dados”	Significa qualquer pessoa física que possa ser identificada, direta ou indiretamente, por meios que provavelmente possam ser utilizados por qualquer pessoa física ou jurídica, em particular por meio da referência a um identificador como um nome, um número de identificação, dados de localização, um identificador online ou a um ou mais fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa.
“Dispositivo”	Significa qualquer objeto programável que possa realizar automaticamente uma sequência de cálculos ou outras operações sobre dados uma vez que tenha sido programado, seja diretamente ou indiretamente, para essa tarefa. Qualquer aparelho eletrônico adaptado para exibir a informação em um formato legível. Os dispositivos incluem, mas não se limitam a, computadores, smartphones, tablets, laptops, servidores, redes, plataformas de telefonia, etc.
EEE	Significa o Espaço Econômico Europeu. Os países que fazem parte do EEE são os Estados membros da UE, assim como a Islândia, o Liechtenstein e a Noruega.
“Autoridade de Supervisão do EEE”	Significa uma autoridade independente de proteção de dados pública que está estabelecida em um Estado membro do EEE..

“Código”	Significa um processo para ofuscar dados transformando-os em uma forma na qual há uma baixa probabilidade de atribuir-lhes um significado ou torná-los legíveis, exceto quando são usados em conjunto com um processo confidencial ou uma chave para decodificá-los. Tal processo pode ser, mas não se limita a, uma função matemática ou um processo algorítmico.
“Administrador da informação”	Significa a pessoa física dentro da organização da Concentrix que, sozinha ou em conjunto com outros, processa ou manipula a informação de acordo com as necessidades, os objetivos, os fins e as regras do Proprietário da Informação.
“Proprietário da informação”	Significa a pessoa física dentro da organização da Concentrix que, sozinha ou em conjunto com outros, determina as necessidades, os objetivos, os fins e as regras de um projeto que inclua o processamento da informação.
“Acordo Intragroupo de Transferência de Dados”	Significa o acordo intra-grupo que compreende o BCR-C e o BCR-P como anexos, que todos os Membros das BCR são obrigados a executar para estarem vinculados pelo BCR-C e pelo BCR-P.
“Sistemas de Informação”	Significa qualquer Dispositivo utilizado direta ou indiretamente por um Usuário ou outro Dispositivo para processar Informação, incluindo, mas não se limitando a, a coleta, gravação, organização, estruturação, armazenamento, adaptação, alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou outra forma de disponibilização, alinhamento ou combinação, restrição, exclusão ou destruição de Dados.
“Líder Local em Privacidade”	Significa a pessoa que é o principal ponto de contato do Oficial de Privacidade de Dados (DPO, na sigla em inglês) e que se encarrega dos assuntos de proteção de dados dentro de cada Membro das BCR.
“Malware”	Significa software que, ao ser introduzido, afeta negativamente a função prevista do software ou hardware. Isso pode incluir, mas não se limita a, vírus, malware, cavalos de Troia, ransomware, etc..

“Redes”	Significa a conectividade física ou lógica que permite que dois ou mais dispositivos se comuniquem.
“Senha” ou “Senha de Frase”	Significa una cadena de caracteres o cualquier otro medio lógico o físico utilizado en conjunto con una Identidad de Usuario durante un proceso de autenticación para probar la identidad de un Usuario y/o otorgar acceso a cierta Información.
“Dados Pessoais”	Significa qualquer informação relacionada a uma pessoa física identificada ou identificável (um Titular de Dados); uma pessoa física identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por meio da referência a um identificador como um nome, um número de identificação, dados de localização, um identificador online ou a um ou mais fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa física. Os Dados Pessoais incluem Dados Pessoais Sensíveis..
“Violação de Dados Pessoais”	Significa uma violação da segurança que leva, de maneira acidental ou ilegal, à destruição, perda, alteração, divulgação não autorizada ou acesso a Dados Pessoais, sejam eles transmitidos, armazenados ou de outro modo processados.
“Comitê de Privacidade”	Significa o comitê interno da diretoria que apoia o Oficial Global de Privacidade de Dados.
“Tratamento” ou “Processamento”	Significa qualquer operação ou conjunto de operações realizadas sobre Dados Pessoais ou sobre conjuntos de Dados Pessoais, seja por meios automatizados ou não, tais como coleta, gravação, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou de outro modo disponibilização, alinhamento ou combinação, restrição, exclusão ou destruição.
“Pseudonimização”	Significa o Tratamento de Dados Pessoais de tal maneira que os Dados Pessoais não possam mais ser atribuídos a um Titular de Dados específico sem o uso de informações adicionais, desde que essas informações adicionais sejam mantidas separadas e estejam sujeitas a medidas técnicas e organizacionais para garantir que os Dados Pessoais não sejam atribuídos a uma pessoa física identificada ou identificável.

“Risco”	Significa um cenário que descreve um evento e suas consequências, estimadas em termos de severidade e probabilidade.
“Gestão de Riscos”	Significa as atividades coordenadas para direcionar e controlar uma organização em relação ao risco..
“Incidente de Seguridad”	Significa acesso ou tentativa de acesso não autorizado ao uso, divulgação, modificação ou destruição de Informação, ou a interferência nas operações do sistema no Sistema de Informação.
“Dados Pessoais Sensíveis”	Significa categorias especiais de Dados Pessoais que, por sua natureza, são particularmente sensíveis em relação aos direitos e liberdades fundamentais, exigindo que esses Dados Pessoais recebam uma proteção específica, uma vez que o contexto de seu Tratamento poderia criar riscos significativos para os direitos e liberdades fundamentais. Esses dados incluem, por exemplo, Dados Pessoais que revelam a origem racial ou étnica, a opinião política, as crenças religiosas ou filosóficas, ou a afiliação sindical, assim como o Tratamento de dados genéticos, dados biométricos com o objetivo de identificar de maneira única uma pessoa física, dados sobre a saúde e dados sobre a orientação sexual de uma pessoa natural.
“Acordo de Serviços”	Significa o acordo celebrado entre uma filial da Concentrix e seu Cliente, em virtude do qual essa filial da Concentrix fornece serviços ao seu Cliente.
“Sub-Encarregado”	Significa a entidade contratada por um Processador de Dados para realizar atividades de processamento específicas em nome do Controlador de Dados, e que está sujeita às mesmas obrigações de proteção de dados estabelecidas no contrato ou outro ato legal entre o Controlador de Dados e o Processador de Dados.
“Software” ou “Aplicação”	Significa qualquer código, instrução, programa ou rotina que permita a manipulação de Dados de maneira direta ou remota através de qualquer meio, e inclui APIs, shells de comandos, etc.
“Transferência de Dados Pessoais.”	Significa o Tratamento, a transferência material ou o acesso remoto a Dados Pessoais a partir de entidades estabelecidas fora do Espaço Econômico Europeu (EEE).
“Usuario”	Significa todos os empregados da Concentrix, terceiros, empregados de terceiros, contratados,

Aprovação Final	empregados de contratados e outras pessoas cuja conduta e funções permitem o acesso aos Sistemas de Informação da Concentrix
“Concentrix” ou “Grupo Concentrix”	Para o BCR e os Procedimentos relacionados, a Concentrix se referirá à Webhelp SAS e a todas as entidades listadas na Lista de entidades vinculadas pelo BCR e que, portanto, são Membros do BCR

CONTROLE DE DOCUMENTO

Versão	Atualização	Resumo das Modificações
0.1	27/02/2022	Aprovação Final
0.2	01/04/2024	Rebranding e formatação Alinhamento com as recomendações EDPB 1/2022 revogação e substituição WP256_Rev01

Frequência de Revisão	Este documento será revisado pelo menos anualmente ou em caso de mudanças
Data de emissão	25/05/2018
Domínio	Privacidade
Classificação	Público
Referência	BCR Apêndice 2 Definições para as BCR e Procedimentos

Apêndice 5

Procedimento a seguir pelo Responsável para o manejo de solicitações e reclamações dos Titulares de Dados

Índice

1. Introdução

A adoção das BCR (por suas siglas em inglês) pelo grupo Concentrix e o compromisso dos membros das BCR em cumprir com isso demonstram o compromisso dos Membros das BCR em fornecer um alto nível de proteção aos Dados Pessoais que processam. A Concentrix se compromete a realizar negócios de acordo com a Legislação Aplicável à Proteção de Dados, incluindo o regulamento Europeu 2016/679 relativo ao processamento de Dados Pessoais a partir de sua data de aplicação. A Concentrix implementou o seguinte procedimento.

Os termos em maiúsculas usados aqui terão o mesmo significado que o especificado no Apêndice 2 das BCR.

2. Objetivos do Procedimento

Os Titulares dos dados, incluindo os funcionários Membros das BCR, são dotados de direitos específicos com relação ao tratamento de seus Dados Pessoais, conforme definido na Seção 7 das BCR. Quando atuarem como responsáveis pelos dados, os Membros das BCR vão assegurar que qualquer solicitação ou reclamação do titular dos dados em relação ao exercício de seus direitos **("Solicitações")** será atendida em um tempo efetivo definido aqui, visando cumprir com as BCR e a Legislação Aplicável à Proteção de Dados.

Este documento descreve como os membros das BCR devem lidar com uma solicitação de um titular de dados quando um membro das BCR atua como Responsável pelos dados (Grupos de interesse, passos e prazos). Quando a solicitação é recebida do titular dos dados e esses dados pessoais são processados por um membro Concentrix BCR em nome de um dos clientes de um membro Concentrix BCR, todas as solicitações devem ser tratadas de acordo com o procedimento especificado e definido no **Apêndice 06 – Procedimentos para o manejo de solicitações do titular dos dados onde a Concentrix atua como encarregada dos dados.**

3. Procedimentos

Como um passo preliminar, os membros das BCR devem expressamente informar aos titulares dos dados que podem exercer seus direitos de acordo com as provisões do artigo 7 das BCR..

3.1 Contato e confirmação de recebimento da solicitação

3.1.1 Procedimento Padrão

Os membros das BCR devem também especificar como esses direitos podem ser exercidos. Para esse propósito, os Membros das BCR devem fornecer ao Titular dos dados meios acessíveis para o exercício de seus direitos e, em particular, um único contato eletrônico dedicado para ser usado independentemente do país onde o

Titular dos dados esteja localizado. Portanto, qualquer solicitação como parte desse processo pode ser enviada diretamente para o seguinte endereço: dpo@concentrix.com – e-mails locais podem ser usados para levar em conta alguma especificação local, como o idioma.

Ao receber uma Solicitação, o Oficial de Privacidade ("DPO") do grupo, ou qualquer outro indivíduo ou entidade, interna ou externa, indicado pelo DPO para o processo de gerenciamento das seguintes responsabilidades, deverá confirmar o recebimento no prazo máximo de 3 dias úteis após o recebimento da solicitação.

3.1.2 Exceção

No caso de uma reclamação recebida por um titular dos dados através de um canal diferente do descrito anteriormente, o membro BCR ou outro órgão que receber a reclamação deverá, imediatamente após ser notificado, entrar em contato com o DPO e (1) serviços postais internos, (2) Líderes de Privacidade Local, (3) Referente de Negócios da Privacidade e (4) departamentos de RH do referido procedimento.

O Oficial de Privacidade do Grupo, ou qualquer outro indivíduo ou entidade, interna ou externa, mencionado pelo DPO para o propósito de gerenciar as seguintes responsabilidades, deverá acusar o recebimento do assunto por escrito dentro de 2 dias úteis após a notificação da função.

3.2 Coleta de Informações

Antes do envio de uma solicitação interna, o Oficial de Privacidade do Grupo, ou qualquer outro indivíduo ou entidade, interna ou externa, designado pelo DPO para o propósito de gerenciar as seguintes responsabilidades, deve (1) garantir que tenha a informação mínima requerida por parte do Titular dos Dados para especificar suas solicitações e (2) se necessário, obter o máximo de informações possível para assegurar que a solicitação seja tratada adequadamente.

Como mínimo, e na medida do possível, deve-se obter as seguintes informações ('**Informação Mínima'**).:

- Aqui está a tradução:
- Nome e sobrenomes dos titulares dos dados; e
- Quando legalmente permitido/necessário, cópia da identificação do Titular dos Dados ou qualquer outro documento exigido como prova de identidade; e
- Detalhes de contato para serem usados ao localizar o Titular dos Dados; e
- Os Dados Pessoais afetados pela Solicitação e o objeto da mesma; e
- Data em que os Dados Pessoais foram inicialmente recebidos; e
- Tipo de direito que o Titular dos Dados deseja exercer (por favor, indique se é acesso, exclusão, bloqueio ou correção).).

Se considerado necessário, membros BCE deverão obter as seguintes informações:

- Claro! Aqui está a tradução:
- Membro BCR que inicialmente coletou os Dados Pessoais; e
- Categoria do tratamento com relação ao qual o titular dos dados está iniciando sua solicitação; e
- Qualquer detalhe relevante à solicitação.

Para obter as informações necessárias, o membro BCR pode convidar o Titular dos Dados, que não especificou informações suficientes em seu e-mail, a completar detalhadamente o documento de questionário, com campos de edição livre, ou qualquer outro meio iniciado pela Concentrix para facilitar a coleta das informações requeridas do Titular dos Dados. (Por exemplo: campos pré-preenchidos no documento, opções disponíveis através de caixas de seleção, etc.) Isso significa autorizar a coleta de dados, no mínimo, indicando (1) se a resposta é obrigatória ou não e (2) as consequências caso a resposta não seja fornecida.

3.3 Análise da solicitação

O Oficial de Privacidade de Dados (DPO), ou qualquer outro indivíduo ou entidade, interna ou externa, designado pelo DPO para o propósito de gerenciar as seguintes responsabilidades, deverá determinar se obteve as informações mínimas para processar a solicitação.

Com base nas informações solicitadas e obtidas, o DPO deverá avaliar a solicitação. Se considerar que a solicitação é razoável e legítima (ao contrário de uma solicitação sem provas de identidade do titular dos dados, uma demanda excessiva que resulte em solicitações repetitivas, solicitações de dados já eliminados de acordo com o período de retenção, solicitações em nome de terceiros, dados futuros de ofícios, etc.), então:

O DPO deverá (i) documentar qualquer solicitação recebida e (ii) realizar a análise relevante da solicitação. Para analisar corretamente a solicitação, o DPO ou qualquer outro indivíduo ou entidade, interna ou externa, designado pelo DPO para gerenciar as responsabilidades anteriores, pode precisar responder às seguintes perguntas:

- Qual é a natureza da solicitação? (acesso, exclusão, objeção, correção, portabilidade);
- Tenho as informações necessárias para identificar o Titular dos Dados?;
- Tenho as informações necessárias com relação ao alcance da solicitação? (geográfico e parâmetros materiais);
- O Titular dos Dados possui os dados solicitados ou tem fácil acesso a eles (por exemplo, através dos sistemas da Concentrix)?;
- A solicitação inclui informações que não estão em um formato claro para os Titulares dos Dados? Em caso afirmativo, certifique-se de que os códigos sejam explicados para que as informações sejam compreendidas;
- A solicitação do Titular dos Dados está baseada em um interesse legítimo?;
- É tecnicamente possível atender à solicitação do Titular dos Dados (particularmente o volume de dados em risco)?;
- Há terceiros envolvidos no tratamento de Dados Pessoais do Titular dos Dados no âmbito da solicitação?;
- O manejo da solicitação poderia implicar que Dados Pessoais de terceiros sejam comunicados ao Titular dos Dados? Em caso afirmativo, é possível extrair apenas os Dados Pessoais do solicitante, com esforços razoáveis e sem risco para os Dados Pessoais de terceiros? Caso contrário, esses Dados Pessoais não podem ser comunicados ao Titular dos Dados.

3.4 Identificação do tipo de resposta

Neste apartado, podem ser contemplados três casos distintos:

3.4.1 Caso 1

Quando as informações fornecidas pelo Titular dos Dados não são suficientes para tratar a solicitação, o DPO, ou qualquer outro indivíduo ou entidade, interna ou externa, designado pelo DPO para o propósito de gerenciar as seguintes responsabilidades, deverá enviar uma solicitação ao Titular dos Dados para informações adicionais, no prazo máximo de 10 dias úteis após o recebimento da solicitação.

Quando a solicitação for muito complexa e sujeita a conformidade com qualquer requisito legal, o prazo de resposta pode ser estendido para até 2 meses, sujeito à documentação da análise de complexidade pelo DPO.

3.4.2 Caso 2

Quando o DPO considerar em sua análise inicial que a solicitação pode **não ser legítima, conforme descrito na seção** 3.7, não deve concluir imediatamente o caso. O Oficial de Privacidade do Grupo, ou qualquer outro indivíduo ou entidade, interna ou externa, designado pelo DPO para o propósito de gerenciar as seguintes responsabilidades, deverá responder ao Titular dos Dados nos próximos 10 dias úteis após o recebimento da solicitação, solicitando ao Titular dos Dados que forneça mais explicações sobre por que ele pretende exercer esses direitos.

Quando necessário, o DPO pode informar grupos de interesse relevantes em nível local e ao Líder Local de Privacidade.

Uma vez recebida uma justificativa adicional com relação à legitimidade da solicitação, o DPO, ou o Líder Local de Privacidade, deve, nos próximos 15 dias úteis após o recebimento das informações do titular dos dados, (1) garantir que responde à solicitação, ou (2) quando ele ou ela considerar durante a primeira análise que a solicitação mencionada pelo Titular dos Dados não é legítima, documentar o motivo pelo qual a solicitação é considerada ilegítima e responder ao Titular dos Dados.

A orientação para a análise de legitimidade da solicitação é fornecida anteriormente para esse procedimento. A resposta deve incluir o motivo pelo qual não foi tomada uma ação e a possibilidade do Titular dos Dados apresentar uma reclamação a uma autoridade de proteção de dados e buscar uma solução judicial.

Quando o DPO ou algum membro relevante da cadeia de privacidade (ou seja, Líder de Privacidade Regional e/ou Local) considerar que, com base nos elementos adicionais, a solicitação pode ser tratada, deverá assegurar que responda ao Titular dos Dados dentro dos 15 dias úteis mencionados anteriormente. Quando a solicitação for muito complexa e sujeita a regulamentação com qualquer requisito legal, o prazo de resposta pode ser estendido para até 2 meses, sujeito à documentação da análise de complexidade pelo DPO.

3.4.3 Caso 3

Quando as informações fornecidas pelo Titular dos Dados forem suficientes, o DPO deverá garantir que a solicitação seja respondida sem demora e no máximo **em 1 mês após o recebimento da solicitação.**

Por favor, tenha em mente que, em qualquer caso, a resposta ao Titular dos Dados deve ocorrer em no máximo 1 mês após o recebimento da solicitação

(exceto em circunstâncias específicas e limitadas já detalhadas neste documento).

3.5 Disposições Locais Mandatórias

O Líder Local de Privacidade, se não for designado diretamente pelo DPO para o processo de gerenciamento das respostas às solicitações recebidas por um membro BCR, deverá estar pronto para cooperar com o DPO, fornecendo-lhe qualquer informação relevante relacionada ao assunto. O DPO deverá então orientar sobre como manejar o caso, considerando as circunstâncias locais, nos 7 dias úteis após o recebimento das informações do Líder Local de Privacidade.

3.6 Processo de escalação

Quando o Titular dos Dados não estiver satisfeito com a resposta inicial dada pelo Líder Local de Privacidade ou pelo DPO, e como resultado do gerenciamento do procedimento descrito anteriormente, esse Titular dos Dados estará autorizado, em qualquer caso, a solicitar imediatamente que sua solicitação seja reexaminada.

O Titular dos Dados deverá fornecer ao membro BCR uma explicação detalhada sobre as partes insatisfatórias da solução previamente fornecida. O DPO informará ao Comitê de Privacidade sobre essa solicitação e permitirá que o Comitê de Privacidade prossiga com a análise da solicitação.

Considerando a análise feita pelo Comitê de Privacidade, e sem revelar essa análise ao Titular dos Dados, o DPO deverá tomar no máximo 2 meses a partir do recebimento da solicitação de reexame para determinar como a solicitação será manejada e informada ao Titular dos Dados por escrito adequadamente.

3.7 Rejeição de uma Solicitação

Embora os membros BCR estejam comprometidos com o manejo eficiente das solicitações dos Titulares dos Dados, sob certas circunstâncias, os membros BCR podem estar autorizados a não aceitar solicitações dos Titulares dos Dados.

Os membros BCR têm o direito de rejeitar uma solicitação de um Titular dos Dados quando, ao acessar tal solicitação, isso possa real ou potencialmente significar que a seguinte informação seja compartilhada com o Titular dos Dados:

- Informação coberta por privilégio legal;
- Informação que um membro BCR está legalmente proibido de comunicar;
- Aquí está a tradução:
- Informação que membros BCR estão processando durante o curso de uma investigação ativa ou procedimento de litígios pendentes.

Quando informações/Dados Pessoais sobre outros Titulares dos Dados forem visíveis, esses dados podem ser redigidos antes de serem compartilhados com o Titular dos Dados.

Além disso, quando o Titular dos Dados se opuser ao tratamento adicional de seus Dados Pessoais e/ou solicitar a exclusão de seus Dados Pessoais, os membros BCR podem negar tal solicitação quando houver uma obrigação legal ou algum interesse prioritário legítimo para que um membro BCR retenha os dados pessoais. Isso deve ser analisado caso a caso e documentado adequadamente.

Em qualquer caso, se uma solicitação ou reclamação do Titular dos Dados for negada por um membro BCR ou se a resposta não for satisfatória, o Titular dos Dados pode entrar em contato com o DPO e/ou pode apresentar diretamente uma reclamação ao seu Órgão de Vigilância competente.

3.8 Comunicação com o Titular dos Dados

Quando se comunicar com o Titular dos Dados, os membros BCR devem cooperar com o Titular dos Dados e atender a qualquer solicitação de forma oportuna. Toda a comunicação deve ser fornecida utilizando uma linguagem clara e simples, em um formato compreensível, conciso e de fácil acesso.

As informações a serem fornecidas ao Titular dos Dados devem ser precisas e limitadas a (i) o que o Titular dos Dados solicitou e (ii) a lista de informações que podem ser fornecidas pelo Responsável pelos Dados de acordo com a Legislação Aplicável de Proteção de Dados.

Como regra geral, os membros BCR não devem aplicar taxas para solicitações razoáveis dos Titulares dos Dados. No entanto, em certas circunstâncias, particularmente quando o manejo da solicitação possa exigir esforços adicionais por parte de um membro BCR, taxas razoáveis, sujeitas a um máximo nacional de acordo com as leis aplicáveis, podem ser aplicáveis, desde que o Titular dos Dados seja informado dessas taxas com antecedência.

-

Questões sobre este procedimento ou conhecimento de qualquer violação ou possível violação do procedimento devem ser relatados diretamente ao Oficial de Privacidade do Grupo.

CONTROL DE DOCUMENTO

Versão	Atualização	Resumo das Modificações
0.1	27/02/2022	Aprovação Final
0.2	19/05/2023	Novo endereço postal da Webhelp SAS / Grupo DPO
0.3	01/04/2024	Rebranding e formatação

Frequência de Revisão	Este documento será revisado pelo menos anualmente ou em caso de mudanças
Data de Emissão	25/05/2018
Domínio	Privacidade
Classificação	Confidencial
Referência	Apêndice BCR 5: Procedimento a ser seguido pelo Responsável para o manejo de solicitações e reclamações dos Titulares dos Dados

Apêndice 6
Procedimento do Responsável para o manejo de solicitações e reclamações dos Titulares de Dados

Tabela de Conteúdos

Introdução

A adoção das BCR (sigla em inglês) e o compromisso dos Membros das BCR em cumpri-las demonstram o empenho dos Membros das BCR em fornecer um alto nível de proteção aos Dados Pessoais que processam. Os Membros das BCR comprometem-se a realizar suas atividades de acordo com a Legislação de Proteção de Dados Aplicável, incluindo o Regulamento Europeu 2016/679 relativo ao processamento de Dados Pessoais a partir de sua data de aplicação, e qualquer normativa relacionada com o processamento de Dados Pessoais aplicável durante a vigência da Política de Privacidade. Consequentemente, a Concentrix implementou o seguinte procedimento.

Os termos em maiúsculas utilizados neste documento terão o mesmo significado que o especificado no Apêndice 2 – Definições de Privacidade para as BCR e Procedimento das BCR.

1.Objetivos do Procedimento

Os Titulares dos dados, incluindo empregados Membros das BCR, têm direitos específicos em relação ao tratamento de seus Dados Pessoais, conforme definido na Seção 7 das BCR.

Quando atuam como Responsáveis pelos Dados, os Membros das BCR garantirão que qualquer solicitação ou reclamação do Titular dos Dados relativa ao exercício de seus direitos ("Solicitações") será atendida dentro de um prazo efetivo definido aqui, com o objetivo de cumprir com as BCR e a Legislação Aplicável à Proteção de Dados. No entanto, isso se aplicará somente quando os Membros das BCR realmente processarem a informação solicitada..

Este documento descreve como os membros das BCR devem gerenciar uma solicitação de um Titular de Dados quando um membro das BCR atua como Responsável pelos dados (Grupos de interesse, etapas e prazos). Quando a solicitação é recebida do Titular dos Dados e esses Dados Pessoais são processados por um Membro das BCR apenas em seu próprio nome, como Responsável pelos Dados, deverão ser tratados de acordo com o procedimento especificamente definido nas Políticas e **Procedimento 05 - Procedimento a ser seguido pelo Responsável para o manejo de solicitações e reclamações dos Titulares de Dados**. Na maioria dos casos, uma solicitação de um indivíduo (por exemplo, um empregado do cliente, usuário final do cliente) se encontrará na seguinte situação:

:

As condições de processamento não cumprem com a Legislação Aplicável de Proteção de Dados (por exemplo, os dados de saúde não são utilizados, armazenados e/ou criptografados de acordo com a legislação de saúde local aplicável;

- O indivíduo deseja exercer seus direitos de privacidade de acordo com a Legislação Aplicável de Proteção de Dados, tais como:
  - Acessar os Dados Pessoais relacionados a ele/ela e processados pelos Membros das BCR em nome do Cliente com o qual estabeleceram uma relação;
  - Obter a retificação, exclusão ou suspensão de qualquer Dado Pessoal impreciso ou incompleto relacionado a ele/ela, ou que não seja mais processado para um propósito válido ou apropriado;
  - Opor-se ao processamento de seus Dados Pessoais a qualquer momento, a menos que tal processamento seja exigido pela legislação aplicável, desde que o indivíduo demonstre ter uma base legítima para se opor em relação à sua situação específica; e
  - Receber seus Dados Pessoais em um formato estruturado, de uso comum e legível por máquina.

Mesmo que esse indivíduo não tenha uma relação direta com a Concentrix, pode haver casos em que os Membros das BCR recebam uma Solicitação diretamente do indivíduo e/ou sejam solicitados pelo Cliente para tratar a Solicitação em seu nome. **Os Membros das BCR devem, em qualquer caso, consultar o compromisso com o Cliente para verificar se há condições específicas para o**

manejo da Solicitação (por exemplo, proibição de se comunicar diretamente com os Titulares dos Dados, etc.).

Como consequência, os custos e os impactos técnicos da Solicitação devem ser antecipados e abordados no início de cada compromisso..

2. Procedimientos

A Concentrix, atuando como Responsável, não é responsável por informar os Titulares dos Dados sobre seus direitos em relação aos Dados Pessoais. A menos que as leis e regulamentos aplicáveis disponham de forma diferente, tais obrigações são de responsabilidade do Responsável pelos Dados. No entanto, os Membros das BCR comprometem-se a fornecer garantias suficientes por meio da implementação de medidas técnicas e organizacionais apropriadas, de modo que o Tratamento de Dados Pessoais em nome do Responsável pelos Dados cumpra com os requisitos aplicáveis e garanta a proteção dos direitos do Titular dos Dados. Portanto, os procedimentos a seguir se aplicam quando a Concentrix atua como Responsável pelos Dados em nome de um Responsável pelos Dados.

Como não se pode excluir formalmente a possibilidade de um Titular dos Dados enviar sua Solicitação diretamente a um Membro das BCR, devem ser considerados dois casos diferentes.

2.1. Solicitação recebida diretamente por um Membro das BCR

2.1.1. Comunicação interna

Qualquer Solicitação relacionada a Dados Pessoais que a Concentrix processe como Responsável pelos Dados (por exemplo, em nome de seus Clientes) recebida por um empregado ou equipe de trabalho de um Membro das BCR deve ser comunicada **imediatamente** ao Líder de Privacidade Local ou ao Referente de Privacidade do Negócio. O Referente de Privacidade do Negócio deverá informar imediatamente ao Líder de Privacidade Local..

Como medida de eficiência, tal Solicitação também pode ser comunicada ao DPO por meio do seguinte e-mail:

dpo@concentrix.com

O DPO atribuirá a Solicitação ao Líder de Privacidade Local correspondente no máximo 1 dia útil após seu recebimento..

As informações fornecidas pelo empregado ou equipe de trabalho da Concentrix devem especificar pelo menos as seguintes informações:

Nome do gerente local responsável pela conta do Cliente;
Cópia da Solicitação; e
Nome do Cliente com o qual o Titular dos Dados está relacionado.

O Referente de Privacidade do Negócio deverá informar imediatamente ao seu Líder de Privacidade Local..

2.1.2. Transferência da Solicitação ao Cliente

Uma vez que receber a Solicitação, o Líder de Privacidade Local redigirá uma comunicação ao Cliente sobre a Solicitação. Essa comunicação deverá (1) ser enviada pelo Líder de Privacidade Local ao Cliente, em cooperação com o gerente local responsável pela relação com o Cliente; e (2) no máximo em 2 dias úteis após

receber a Solicitação. O Líder de Privacidade Local também informará ao DPO que a Solicitação foi transferida ao Cliente.

2.1.3. Assistência do Membro das BCR ao Cliente

Ao mesmo tempo, o Líder de Privacidade Local, com o apoio das equipes de operações e gestão de contas, deverá avaliar e verificar se a Concentrix realmente processa os Dados Pessoais do Titular dos Dados que apresenta a Solicitação.

Nenhuma resposta será fornecida sem as instruções do Cliente.

Caso o Cliente permita que os Membros das BCR manejem a Solicitação em seu nome, o Líder Local do Membro das BCR deverá determinar com o Cliente se o próprio Cliente ou o Membro das BCR deverá acusar o recebimento da Solicitação e informar o Titular dos Dados sobre o papel do Membro das BCR no processamento de sua Solicitação.

A menos que o Cliente indique o contrário de forma expressa, os Membros das BCR não deverão contatar o Titular dos Dados durante todo o procedimento.

2.2. Solicitação enviada pelo Responsável pelos Dados a um Membro das BCR

2.2.1. Comunicação interna

Qualquer Solicitação relacionada a Dados Pessoais que a Concentrix processe como Responsável pelos Dados (por exemplo, em nome de seus Clientes) recebida por um empregado ou equipe de trabalho de um Cliente deve ser comunicada imediatamente ao Líder de Privacidade Local ou ao Referente de Privacidade do Negócio. O Referente de Privacidade do Negócio deverá informar imediatamente ao seu Líder de Privacidade Local.

Quando um Cliente enviar a um Membro das BCR uma Solicitação do Titular dos Dados sobre o processamento de seus Dados Pessoais para que a gerencie, o Membro das BCR deverá acusar o recebimento da mesma ao Cliente no máximo em 2 dias úteis após receber a Solicitação.

No máximo em 5 dias úteis após o recebimento da Solicitação, o Membro das BCR deverá verificar o grau em que pode atender e gerenciar a Solicitação.

2.3. Análise da Solicitação

Após o recebimento de uma Solicitação, seja diretamente do Titular dos Dados ou do Cliente, e sujeito às disposições e etapas descritas neste Procedimento, o Líder de Privacidade Local, ou qualquer outra pessoa ou entidade, interna ou externa, designada pelo Líder de Privacidade Local para o propósito de gerenciar as seguintes tarefas, deverá garantir e verificar que possui todas as informações necessárias do Cliente e do Titular dos Dados para atender à sua Solicitação, em particular:

A informação fornecida permite ao Membro das BCR identificar o Titular dos Dados? (ou seja, nome e sobrenome do Titular dos Dados);
Descrição do contexto em que os Dados Pessoais foram coletados (se possível)
O Membro das BCR está autorizado a gerenciar a Solicitação em nome do Cliente?

Qual é a natureza da Solicitação? (acesso, exclusão, oposição, retificação, portabilidade) Qual é a natureza da Solicitação? (acesso, exclusão, oposição, retificação, portabilidade)

O Cliente considera que a Solicitação do Titular dos Dados é razoável?

É tecnicamente possível atender à Solicitação do Titular dos Dados (considerando especialmente o volume de dados em questão)?

O Membro das BCR tem informações suficientes sobre o escopo da Solicitação? (escopo geográfico e material, data aproximada em que os dados foram coletados)

O Titular dos Dados possui os dados solicitados ou tem fácil acesso a eles?

A solicitação inclui informações que não estão em um formato claro para os Titulares dos Dados? Caso afirmativo, garantir que os códigos sejam explicados para que a informação seja compreendida;

Há terceiros envolvidos no tratamento de Dados Pessoais do Titular dos Dados dentro do âmbito da solicitação?

O tratamento da solicitação poderia implicar que Dados Pessoais de terceiros sejam comunicados ao Titular dos Dados? Em caso afirmativo, é possível extrair apenas os Dados Pessoais do solicitante, com esforços razoáveis e sem risco para os Dados Pessoais de terceiros?

É importante destacar que a coleta dessa informação deve ser limitada ao que está atualmente disponível na Concentrix. Não será coletada informação adicional.

Os Membros das BCR **deverão se abster, na medida do possível, de se comunicar diretamente com o Titular dos Dados, mesmo que o Cliente solicite. Quando tal solicitação for enviada a um Membro das BCR, este deverá primeiro discutir com o Cliente a real necessidade de que a Concentrix estabeleça contato direto com o Titular dos Dados. Se o Membro das BCR aceitar contatos diretos com o Titular dos Dados, esse Membro das BCR deverá informar ao Cliente que este último mantém toda a responsabilidade perante o Titular dos Dados para gerenciar adequadamente a Solicitação.**

Identificação do tipo de resposta

O Líder de Privacidade Local deverá garantir que a informação fornecida pelo Cliente e pelo Titular dos Dados seja examinada dentro dos 8 dias úteis seguintes ao recebimento da Solicitação para determinar se:

Possui as informações apropriadas para gerenciar a Solicitação; e

Considera que a Solicitação é razoável (diferente de uma Solicitação sem prova de identidade do Titular dos Dados, uma demanda excessiva resultante de Solicitações repetitivas, Solicitações de Dados Pessoais já excluídos de acordo com o período de retenção, Solicitações em nome de terceiros, etc).

(IV)**A seguir, são possíveis três casos. São os seguintes:**

(v) **Caso 1**

Quando as informações fornecidas pelo Titular dos Dados não forem suficientes para gerenciar a solicitação, o Líder de Privacidade Local, ou qualquer outro indivíduo ou entidade, interna ou externa, designada pelo Líder de Privacidade Local para gerenciar as seguintes responsabilidades, deverá enviar uma solicitação ao Cliente para obter informações adicionais no máximo 2 dias úteis após o recebimento da solicitação.

Quando a solicitação for muito complexa e sujeita a conformidade com qualquer requisito legal, o prazo de resposta pode ser estendido **até 20 dias úteis**, sujeito à documentação da análise de complexidade pelo Líder de Privacidade Local.

(vi) **Caso 2**

Quando o Líder de Privacidade Local considerar em sua análise inicial que a solicitação pode **não ser razoável**, não deve concluir o caso imediatamente. O Líder de Privacidade Local, ou qualquer outro indivíduo ou entidade, interna ou externa, designada pelo Líder de Privacidade Local para gerenciar as seguintes responsabilidades, deverá responder ao Cliente **nos próximos 10 dias úteis** após o recebimento da solicitação, solicitando ao Cliente que forneça mais informações sobre o motivo pelo qual o Titular dos Dados deseja exercer esses direitos.

Solicitação apresentada pelo Titular dos Dados não é razoável, o Líder de Privacidade Local deverá documentar o motivo pelo qual considera que a Solicitação não é razoável e deverá garantir, após a aprovação escrita do DPO, responder ao Cliente ou ao Titular dos Dados, se assim instruído expressamente pelo Cliente, no máximo **15 dias úteis** após o recebimento das informações adicionais.

A resposta deverá incluir o motivo pelo qual nenhuma ação está sendo tomada e a possibilidade para o Titular dos Dados de apresentar uma reclamação a uma autoridade de proteção de dados e buscar um recurso judicial. A redação dessa resposta deverá ser validada pelo DPO e pelo Cliente.

Quando o Líder de Privacidade Local considerar que, com base nas informações adicionais, a Solicitação pode ser atendida, deverá garantir que a solicitação seja tratada dentro dos **15 dias úteis** mencionados anteriormente e deverá informar o DPO em conformidade.

(vii) **Caso 3**

Quando as informações fornecidas pelo Cliente e/ou pelo Titular dos Dados forem suficientes, o Líder de Privacidade Local deverá garantir que a resposta à Solicitação seja dada, de acordo com as instruções do Cliente, dentro dos 15 dias úteis seguintes ao seu recebimento e deverá informar por escrito ao DPO sobre o prazo e o conteúdo da resposta fornecida.

2.3.1. Processo de Escalonamento

No caso de uma reclamação recebida diretamente do Titular dos Dados sobre como sua Solicitação foi tratada, seja durante ou após a resposta, o Líder de Privacidade Local deverá garantir que compartilhe o assunto com o Cliente e o DPO, **no máximo 3 dias úteis** após o recebimento da reclamação do Titular dos Dados.

ara cada um dos passos anteriores, e quando necessário para tratar o caso adequadamente, o Líder de Privacidade Local deverá estar disposto a cooperar com o DPO fornecendo a ele qualquer informação relevante em relação ao assunto e informar ao Cliente sobre o andamento do procedimento.

A orientação do Oficial de Proteção de Dados do Grupo será vinculativa. No entanto, o DPO não deverá contatar diretamente o Titular dos Dados, a menos que o Cliente e o Líder de Privacidade Local solicitem expressamente.

2.3.2. Rejeição de uma Solicitação

Embora os Membros das BCR estejam comprometidos em gerenciar as Solicitações dos Titulares dos Dados de maneira eficiente, em certas circunstâncias, como definido a seguir, os Membros das BCR podem ter o direito de não aceitar a Solicitação do Cliente ou do Titular dos Dados.

Os Membros das BCR podem se opor à Solicitação do Cliente ou do Titular dos Dados quando aceitar a Solicitação implicar que será compartilhada a seguinte informação:

Informação coberta por privilégio legal;
Informação que um Membro das BCR está legalmente proibido de divulgar; e/ou
Informação que um Membro das BCR está processando durante o curso de uma investigação em andamento ou procedimento judicial pendente.

Quando houver um conflito de privacidade, os Dados Pessoais podem ser redigidos antes de serem compartilhados com o Cliente ou o Titular dos Dados.

Além disso, no caso de uma Solicitação recebida do Cliente relacionada a um Titular dos Dados que se opõe ao processamento adicional de seus Dados Pessoais e/ou solicita a exclusão de seus Dados Pessoais, os Membros das BCR podem rejeitar tal Solicitação quando obrigações legais impedirem os Membros das BCR de atendê-la ou quando os Membros das BCR tiverem um interesse legítimo preponderante. Isso deverá ser avaliado caso a caso e submetido ao DPO para uma decisão final antes de informar o Cliente ou o Titular dos Dados.

2.4. Comunicação com o Titular dos Dados

Se o Cliente exigir que os Membros das BCR gerenciem a Solicitação em seu nome, as seguintes regras se aplicarão quando os Membros das BCR se comunicarem com o Titular dos Dados.

Sob nenhuma circunstância e a menos que o Cliente indique expressamente, os Membros das BCR deverão contatar o Titular dos Dados durante todo o procedimento. Mesmo que solicitado pelo Cliente, os Membros das BCR deverão se abster, na medida do possível, de se comunicar com o Titular dos Dados.

Ao se comunicar com o Titular dos Dados, os Membros das BCR deverão cooperar com o Titular dos Dados e atender a qualquer Solicitação de maneira oportuna. Toda comunicação deve ser fornecida utilizando uma linguagem clara e simples, de forma inteligível, concisa, facilmente acessível e compreensível.

A informação que deve ser fornecida aos Titulares dos Dados deve ser precisa e limitada a (i) o que o Titular dos Dados solicitou e (ii) a lista de informações que podem ser fornecidas por um Responsável pelos Dados de acordo com a Legislação Aplicável de Proteção de Dados.

O Líder de Privacidade Local deverá prestar atenção especial aos prazos mencionados neste Procedimento.

Como regra geral, os Membros das BCR não deverão aplicar tarifas para Solicitações razoáveis dos Titulares dos Dados. No entanto, em certas circunstâncias, particularmente quando o manejo da Solicitação envolver esforços significativos por parte dos Membros das BCR, tarifas razoáveis poderão ser

aplicadas, sujeitas a um limite nacional de acordo com as leis aplicáveis, desde que o Titular dos Dados seja informado sobre tais tarifas com antecedência.

-

Perguntas sobre este procedimento ou o conhecimento de qualquer violação ou potencial violação do procedimento devem ser relatados diretamente ao Oficial de Proteção do Grupo.

-

CONTROLE DE DOCUMENTO

Versão	Atualização	Resumo das Modificações
0.1	27/02/2022	Aprovação Final
0.2	19/05/2023	Novo endereço postal da Webhelp SAS / Grupo DPO
0.3	01/04/2024	Rebranding e Formatação

Frequência de Revisão	Este documento será revisado pelo menos anualmente ou em caso de alterações.
Data de Emissão	25/05/2018
Domínio	Privacidade
Classificação	Confidencial
Referência	Apêndice BCR 5: Procedimento do Encargado para o manejo de solicitações e reclamações dos Titulares de Dados

Apêndice 11A
Abrangência do material das BCR para o Responsável

Lista de Finalidades do Tratamento e Categorias relacionadas de Dados Pessoais e Titulares dos Dados

Além das disposições da seção 2.1 sobre o escopo material destas BCR-C, a tabela abaixo fornece mais detalhes sobre as Transferências realizadas sob estas BCR-C. Esta tabela detalha a Finalidade do Tratamento e as categorias relacionadas de Titulares dos dados e Dados Pessoais cobertos por estas BCR-C. A tabela fornecida na seção 1 abaixo oferece detalhes sobre as transferências de dados pessoais realizadas entre os Membros das BCR listados no Apêndice 1 sob estas BCR-C.

Os países para os quais os Dados Pessoais podem ser transferidos dependem da localização dos Membros das BCR envolvidos nas atividades de Tratamento e são fornecidos no Apêndice 1. Vale notar que, no que diz respeito às BCR-C, as Transferências de Dados Pessoais ocorrem principalmente entre os Membros das BCR de uma mesma Região (exceto para as entidades Globais, onde pode haver transferências entre essas entidades Globais e todos os outros Membros das BCR, dependendo das Finalidades do Tratamento). Para maior transparência, incluímos uma tabela adicional que apresenta as Regiões na seção 2 deste Apêndice.

1.Tabela sobre as Transferências de Dados Pessoais entre os Membros das BCR listados no Apêndice 1 sob estas BCR-C

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
Atividades de tratamento de RH	**Gestão de recrutamento**	**1.Dados de identificação** (por exemplo, nome, sobrenome, e-mail, número de telefone, foto (se fornece), endereço) **2Dados econômicos e financeiros** (por exemplo, expectativas salariais) **3. Dados profissionais** (por exemplo, currículo, experiência anterior,	**Candidatos**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
		diplomas, certificados, idiomas estrangeiros falados, avaliação de conhecimentos e formações, número e cópia da sua carteira de habilitação) de trabalho (somente se necessário) **4. Verificação de antecedentes** (resultados da verificação de antecedentes (apenas os resultados e para candidatos aprovados que forem contratados)	
	Gestão de registros de empregados (inclui o processo de integração, manutenção do registro de empregados de acordo com a legislação aplicável, acompanhamento administrativo da medicina ocupacional, diretório interno)	**1. Dados de identificação** (por exemplo, nome, sobrenome, e-mail, número de telefone, foto do titular dos dados, endereço, gênero, estado civil) **2. Dados profissionais** (por exemplo, currículo, histórico educacional e informações sobre habilidades do empregado, experiência anterior, diplomas/certificados, idiomas estrangeiros falados, avaliação de conhecimentos e formações, número e cópia da sua carteira de trabalho (somente se necessário), número	**Empleados de los Miembros de las BCR**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
		de identificação interna do empregado, localização do escritório, histórico de trabalho anterior, unidade de negócios/divisão, chefe direto, tipo de contrato, número de segurança) **3. Dados econômicos e financeiros** (por exemplo, renda/salário,IBAN/BIC) **4. Dados sensíveis** (número de segurança social)	
	Gestão de folha de pagamento	**1. Dados de identificação** (por exemplo, nome, sobrenome, e-mail, número de telefone, endereço) **2. Dados profissionais** (por exemplo, número de identificação interna do empregado, tipo de contrato, horas de trabalho) **3. Dados econômicos e financeiros** (por exemplo, dados de pagamento (horas trabalhadas, ausências, compensações e benefícios, bonificações, dados sobre benefícios e	**Empregados dos Membros das BCR**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
		direitos), salário), IBAN/BIC) **4. Dados sensíveis** (número de Segurança Social))	
	Gestão do programa de indicações	**1. Dados de identificação** (por exemplo, nome, sobrenome, e-mail, número de telefone, endereço) **2. Dados profissionais** (por exemplo, currículo, experiência anterior, diplomas, certificados, idiomas estrangeiros falados, avaliação de conhecimentos e formações).	**Empregados dos Membros das BCR** **Candidatos**
	Gestão de crachás para empregados	**1. Dados de identificação** (por exemplo, nome, sobrenome, número de telefone) **2. Dados profissionais** (por exemplo, função do cargo, número de identificação interna do empregado), número de identificação do empregado, áreas autorizadas e horas de trabalho) **3. Dados econômicos e financeiros** (por exemplo, pagamento	**Empregados dos Membros das BCR**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
		relacionado ao uso do refeitório)	
	Gestão da formação de empregados (inclui formação interna e formação para clientes)	**1. Dados de identificação** (por exemplo, nome, sobrenome, e-mail, número de telefone, endereço) **2. Dados profissionais** (por exemplo, título do cargo, número de identificação interna do empregado, informações sobre formação (tipo de formação, data, presença, resultados de testes, etc.), localização do escritório, histórico de trabalho anterior, unidade de negócios/divisão, chefe direto)	**Empregados dos Membros das BCR**
	Gestión de la carrera y movilidad de empleados	**1. Datos de identificación** (por ejemplo, nombre, apellidos, correo electrónico, número de teléfono, foto (si se proporciona), dirección) **2. Datos profesionales** (por ejemplo, CV, título del puesto actual, experiencia previa, diplomas, certificados, idiomas	**Empregados dos Membros das BCR**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
		extranjeros hablados, evaluación de conocimientos y formaciones, número y copia de su permiso de trabajo (solo si es necesario))	
	Verificação de antecedentes de empregados	**1. Dados de identificação** (por exemplo, nome, sobrenome, e-mail, número de telefone, foto (se fornecida), endereço) **2. Dados profissionais (**por exemplo, currículo, título do cargo atual, experiência anterior, diplomas, certificados, idiomas estrangeiros falados, avaliação de conhecimentos e formações, número e cópia da sua carteira de trabalho (somente se necessário) **3. Informações da verificação de antecedentes** (por exemplo, resultados da verificação de antecedentes)	**Empregados dos Membros das BCR**
	Gestão de ausências e tempo de trabalho de empregados	**1.Dados de identificação** (por exemplo, nome, sobrenome) **2.Dados profissionais** (por	**Empregados dos Membros das BCR**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
		exemplo, número de identificação interna) del empregado, localização do escritório, histórico de trabalho anterior, unidade de negócios/divisão, chefe direto, tipo de contrato, horas de trabalho, horário de trabalho, ausências (permissões por doença, férias, etc.)	
	Gestão de escolhas profissionais	**1. Dados de identificação** (por exemplo, nome, sobrenome, idade) **2. Dados profissionais** (por exemplo, preparação da lista eleitoral (identidade dos eleitores, idade, tempo de serviço, escola), gestão das solicitações (identidade, natureza do mandato solicitado, informações para verificar o cumprimento dos requisitos de elegibilidade), se aplicável, filiação sindical declarada pelos candidatos) e publicação dos resultados das eleições (identidade dos candidatos, mandatos afetados, número e percentual de votos obtidos,	**Empregados dos Membros das BCR**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
		identidade dos empregados eleitos e, se aplicável, filiação sindical dos empregados eleitos).	
	Gestão dos comitês dos órgãos de representação dos empregados	**1. Dados de identificação** (por exemplo, nome, sobrenome) **2. Dados profissionais** (por exemplo, convocações, documentos preparatórios, relatórios, diversas atas dos comitês dos órgãos de representação)	**Empregados dos Membros das BCR**
	Gestão de desempenho e avaliação de empregados	**1. Dados de identificação** (por exemplo, nome, sobrenome). **2. Dados profissionais** (por exemplo, informações sobre a avaliação: datas das entrevistas de avaliação, identidade do avaliador, competências profissionais do empregado, objetivos atribuídos, resultados esperados,	**Empregados dos Membros das BCR**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
		resultados obtidos, avaliação) de habilidades profissionais baseadas em critérios objetivos com uma ligação direta e necessária com o cargo, observações e desejos formulados pelo empregado, previsões de desenvolvimento profissional. Para os agentes, a transcrição das conversas telefônicas com o cliente final pode ser utilizada para fins de avaliação de qualidade.	
	Avaliação de qualidade dos Game-Changers	**1. Dados de identificação** (por exemplo, nome, sobrenome, e-mail) **2. Dados profissionais** (por exemplo, número de identificação interna do empregado, título do cargo, chefes diretos, KPIs, objetivos atribuídos, resultados esperados, resultados obtidos, avaliação de habilidades) profissionais baseadas em critérios objetivos com uma ligação direta e necessária com o cargo,	**Agentes / operadores dos Membros das BCR**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
		observações e desejos formulados pelo empregado, previsões de desenvolvimento profissional. A transcrição das conversas telefônicas com o cliente final pode ser utilizada para fins de avaliação de qualidade, resultados da avaliação.	
	Programa de Bem-Estar dos Empregados	**1. Dados de identificação** (por exemplo, nome, sobrenome, e-mail) **2. Dados profissionais** (por exemplo, número de identificação interna, pontuação de pesquisas, conversas de acompanhamento programadas, cargo, chefe direto, turnos, horas de trabalho, resultados de avaliação de qualidade, etc.)	**Empregados dos Membros das BCR (moderadores)**
	Gestão do programa de **Impact Sourcing (recrutamento, relatórios, etc.)**	**1. 1. Dados de identificação** (por exemplo, nome, sobrenome, e-mail, número de telefone, foto (se fornecida), endereço) **2. Dados econômicos e financeiros** (por exemplo,	**Candidatos,** **Empregados dos Membros das BCR**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
		expectativas salariais) **3. Dados profissionais** (por exemplo, currículo, experiência anterior, diplomas, certificados, idiomas estrangeiros falados, avaliação de conhecimentos e formações, número e cópia da sua carteira de trabalho (somente se necessário), fonte de recrutamento)	
	Gestão de viagens e despesas	**1. 1. Dados de identificação** (por exemplo, nome, sobrenome, **endereço)** **2. Dados profissionais** (por exemplo, título do cargo, número de identificação interna do empregado, reserva de reserva, datas de viagem, justificativa da viagem de negócios, chefe direto)3. Datos económicos y financieros (por exemplo, relatório de despesas, faturas, IBAN / BIC)	**Empregados dos Membros das BCR**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
	Gestão de atividades sociais e culturais	**1. Dados de identificação** (por exemplo, nome, sobrenome, endereço, estado civil/relacionamento) **2. Dados profissionais** (por exemplo, título do cargo, número de identificação interna do empregado) **3. Dados econômicos e financeiros** (por exemplo, rendimentos, benefícios e compensações solicitados e fornecidos)	**Empregados dos Membros das BCR (e seus familiares declarados)**
Vida e serviços da empresa	**Gestão de TI (atribuição e gestão de equipamentos de informática, serviço de suporte técnico)**	**1. Dados de identificação** (por exemplo, nome, sobrenome, endereço de e-mail) **2. Dados profissionais** (por exemplo, número de identificação interna do empregado, título do cargo, localização do escritório, chefe direto, informações sobre a solicitação de TI (número do ticket, assunto da solicitação, acompanhamento da solicitação) **3. Dados técnicos e de conexão** (por exemplo, endereço	**Empregados dos Membros das BCR**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
		IP, informações da conta de usuário, ID do dispositivo, aplicativos profissionais necessários e sites)	
	Segurança da informação interna (prevenção de fraudes)	**1. 1. Dados de identificação** (por exemplo, nome, sobrenome, endereço de e-mail) **2. Dados profissionais** (por exemplo, número de identificação interna do empregado, título do cargo, localização do escritório, chefe direto) **3. Dados técnicos e de conexão** (por exemplo, endereço IP, informações da conta de usuário, ID do dispositivo, alertas, resultados dos alertas)	**Empregados dos Membros das BCR**
	CCTV nas instalações da Concentrix	**1. Dados de identificação** (por exemplo, gravações)	**Empregados dos Membros das BCR** **Visitantes nas instalações dos Membros das BCR**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
	Gestão da telefonia no local de trabalho	**1. Dados de identificação:** (por exemplo, nome, sobrenome, endereço de e-mail, número de telefone) **2. Dados técnicos e de conexão** (por exemplo, endereço IP, inícios de sessão, dados do ID do dispositivo, tipo de telefone, informações relevantes sobre o uso de serviços de telefonia e dados necessários para fins de faturamento, incluindo operador, natureza da chamada (local, nacional, internacional), duração da chamada, hora e data de início e término da chamada e fatura	**Empregados dos Membros das BCR**
	Comunicação interna aos empregados (incluindo comunicação interna por e-mail ou através de redes privadas virtuais (intranet)	**1. Dados de identificação** (por exemplo, nome, sobrenome, endereço de e-mail). **2. Dados profissionais** (por exemplo, gráficos, áreas de discussão, áreas de informação, aplicativos e redes). **3. Dados técnicos e de conexão** (por exemplo, endereço	**Empregados dos Membros das BCR**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
		IP, dados do ID do dispositivo, informações da conta de usuário).	
	Pesquisa e formulário para empregados	**1. Dados de identificação** (por exemplo, nome, sobrenome, endereço de e-mail, número de telefone) **2. Dados técnicos e de conexão** (por exemplo, número de identificação interna do empregado, título do cargo, função, localização do escritório, resultados anônimos e agregados).	**Empregados dos Membros das BCR**
	Diretório interno e gestão de acesso e contas de usuários dos empregados	**1. 1. Dados de identificação** (por exemplo, nome, sobrenome, endereço de e-mail) **2. Dados profissionais** (por exemplo, gráficos, funções, áreas de atuação) Áreas de discussão, áreas de informação, aplicações e redes. **3. Dados técnicos e de conexão** (por exemplo, endereço IP, dados do ID do	**Empleados de los Miembros de las BCR**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
		dispositivo, informações da conta de usuário)	
	Acesso à Internet e controle e prevenção de perda de dados	**1. Dados de identificação** (por exemplo, nome, sobrenome, endereço de e-mail). **2. Dados profissionais** (por exemplo, número de identificação interno do funcionário, cargo, função, localização do escritório, gerente direto, aplicativos e sites autorizados, cargo do funcionário). **3. Dados técnicos e de conexão** (por exemplo, endereço IP, dados do ID do dispositivo, informações da conta de usuário)	**Funcionários dos Membros das BCR**
Legal / Cumprimento	**Prevenção e detecção de fraudes**	**1. Dados de identificação** (por exemplo, nome, sobrenome, e-mail, número de telefone). **2. Dados técnicos e de conexão** (por exemplo, endereço IP, logins, dados do ID do dispositivo, dados de interação, relatórios de erros, informações de	**Empregados dos Membros das BCR** **Empregados dos Membros das BCR**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
		monitoramento incorporadas no aplicativo, dispositivo utilizado. **3. Dados de interação necessários para investigar uma possível fraude** (por exemplo, identificação através dos meios utilizados para fornecer os serviços e contatar os clientes finais; dados de voz do cliente final e do funcionário do prestador de serviços, Transcrição da interação; número de telefone, endereço de e-mail, planejamento de operações, indicadores de desempenho de operações e indicadores de desempenho dos colegas.	
	Sistema de denúncias	**1. Dados de identificação** (por exemplo, nome, sobrenome, e-mail, número de telefone, detalhes das pessoas que fizeram a denúncia, das pessoas objeto da denúncia e das pessoas envolvidas no processamento da denúncia).	**Empleados y administradores de los Miembros de las BCR**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
		2. Dados profissionais (por exemplo, tipo de contrato, cargo, função/trabalho da(s) pessoa(s) que reportaram o incidente, da(s) pessoa(s) implicadas no incidente e da(s) pessoa(s) envolvidas na investigação) **3. Informações da denúncia** (por exemplo, fatos reportados, evidências como parte da investigação, registro dos acompanhamentos da investigação da denúncia).	
	Gestão de entidades corporativas e legais *(incluindo mandatos e poderes, delegação de poderes e assinaturas, relatórios corporativos (reuniões, comitês), associações profissionais, diretório de consultores externos*	**1. Dados de identificação** (por exemplo, nome ou razão social, e-mail, número de telefone) **2. Dados profissionais** (por exemplo, currículo, registros educacionais e informações sobre as habilidades do funcionário, experiência prévia, diplomas/certificados, idiomas falados, avaliação de conhecimentos e treinamentos, número e cópia da autorização de	**Empleados y administradores de los Miembros de las BCR**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
		trabalho (somente se necessário), número de identificação interno do funcionário, localização do escritório, delegação de autoridades, procurador). **3. Dados econômicos e financeiros** (por exemplo, pagamentos, receitas/salário, situação financeira, faturas, número do cartão de crédito) , IBAN/BIC).	
	Procedimentos de litígios e disciplinares dos funcionários	**1. Dados de identificação** (por exemplo, nome, sobrenome, e-mail, número de telefone, gravações (se necessário), endereço) **2. Dados profissionais** (por exemplo, número de identificação interno do funcionário, localização do escritório, gerente direto, informações relacionadas a possíveis ações disciplinares e procedimentos para funcionários,	**Funcionários dos Membros das BCR** **Advogados**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
		natureza do litígio relacionado aos negócios, cargo/função) **3. Informações relacionadas ao assunto do litígio** (por exemplo, tema, riscos estimados, evidências, etc.).	
	Gestão de litígios	**1. Dados de identificação** (por exemplo, nome, sobrenome, e-mail, número de telefone, gravações (se necessário), endereço). **2. Dados profissionais** (por exemplo, natureza do litígio relacionado aos negócios, cargo/função). **3. Informações relacionadas ao assunto do litígio** (por exemplo, tema, riscos estimados, evidências, etc.)	**Funcionários dos Membros das BCR** **Parceiros comerciais dos membros das BCR** **Advogados**
	Clients and business partners database (empresa a empresa)	**1. Dados de identificação** (por exemplo, nome ou razão social, e-mail, número de telefone, endereço da sede). **Dados profissionais** (por exemplo, cargo/ função). **3Dados econômicos e financeiros** (por	**Socios comerciales/clientes de los miembros de las BCR**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
		exemplo, pagamentos, receitas/salário, situação financeira, faturas, número do cartão de crédito, IBAN/BIC).	
Operações e Marketing	**Gestão de clientes e prospects**	**1. Dados de identificação** (nome, sobrenome, e-mail, número de telefone, endereço profissional). **2. Dados profissionais** (cargo, função, nome da empresa, localização do escritório) 3. Dados econômicos e financeiros (acordo com o cliente, fatura, requisitos de pagamento, ordens de compra)	**Clientes/prospects dos membros das BCR (contato comercial)**
	Campanhas de marketing direto da Concentrix	**1. Dados de identificação** (nome, sobrenome, e-mail, número de telefone, endereço profissional). **2. Dados profissionais** (cargo, função, nome da empresa, localização do escritório, decisão do resultado)	**Clientes/prospects dos membros das BCR (contato comercial)**
	Processamento de Serviços de Pagamento – WPS	**1. Dados de identificação** (por exemplo, nome, sobrenome, documento de identidade, e-mail,	**Clientes/prospects dos membros das BCR (contato comercial)**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
		número de telefone, endereço postal, gênero, referências internas) **2. Dados profissionais** (por exemplo, informações relacionadas à profissão, informações sobre a qualificação regulatória de uma pessoa exposta politicamente) **3. Dados econômicos e financeiros** (por exemplo, pagamentos, receitas/salário, situação financeira, faturas, IBAN/BIC).	
Relacionamentos com parceiros/fornecedores	**Gestão de fornecedores e gestão de contratos**	**1. Dados de identificação** (por exemplo, nome, e-mail, número de telefone, endereço da sede). **Dados profissionais** (por exemplo, cargos, cópias de acordos com fornecedores, faturas, requisitos de pagamento, ordens de compra)	**Funcionários dos Membros das BCR** **Contato comercial do fornecedor**

Âmbito das atividades de tratamento	Finalidade do tratamento	Categorias de dados pessoais	Categorias de Titulares dos Dados
	Gestão de relacionamentos com corretores de dados	**1. Dados de identificação** (por exemplo, nome, e-mail, número de telefone, endereço). **2. Dados profissionais** (por exemplo, cargo/função, gerente direto, opção de inclusão/exclusão, interesses, relação contratual, fatura, requisitos de pagamento).	**Funcionários dos Membros das BCR** **Contato comercial do fornecedor Cliente/Prospects de Webhelp (contato comercial)**

2. Tabela sobre as regiões dos Membros das BCR

Concentrix Geo/ Regiões	Países incluídos na geografia/região

Grupo (Global)	**Todos os países*** *As transferências podem ocorrer entre entidades globais (incluindo entidades de Serviços Compartilhados Globais) e todas as demais entidades membros das BCR do grupo, independentemente do país de localização identificado no Apêndice 1.
AMERICAS	**Canadá** **Colômbia** **El Salvador** **Guatemala** **Honduras** **México** **Nicarágua** **Peru** **EUA**
APAC	**Austrália** **China** **Hong Kong** **Japão** **Malásia** **Filipinas** **Cingapura** **Tailândia**
CRIT	**Albânia** **República Tcheca** **Itália** **Eslováquia**

DACH	**Áustria** **Bósnia e Herzegovina** **Bulgária** **Alemanha** **Hungria** **Kosovo** **Macedônia do Norte** **Polônia** **Eslovênia** **Suíça**
FRANÇA	**Argélia** **Benin** **França** **Grécia** **Costa do Marfim** **Madagascar** **Marrocos** **Portugal** **Romênia** **Senegal**
MET	**Egito** **Israel** **Jordânia** **Arábia Saudita** **Turquia**
PAÍSES BAIXOS	**Países Baixos** **Suriname**
NORDICS	**Dinamarca** **Estônia** **Finlândia** **Letônia** **Lituânia** **Noruega** **Suécia**

ESPANHA	Espanha
UK	**Índia** **África do Sul** **Reino Unido**
WPS/WKS	**Bélgica** **França** **Alemanha** **Itália** **Portugal** **Espanha** **Reino Unido** **Estados Unidos** **Estados Unidos** *As transferências só podem ser realizadas entre afiliados da WPS/WKS.*
NETINO	**França** **Madagascar**
WEBHELP MEDICA	**França** **Portugal** **Espanha** As transferências só podem ser realizadas entre afiliados da Webhelp Medica

CONTROL DE DOCUMENTO

Versão	Atualização	Resumo das modificações
0.1	27/02/2022	Aprovação final
0.2	19/05/2023	Controle de documentos (adicionado) Atualização de países e regiões Novo processamento adicionado (programa de bem-estar)
0.3	01/04/2024	Rebranding e formatação

Frequência de revisão	Este documento será revisado pelo menos uma vez ao ano ou quando ocorrerem mudanças
Data de emissão	25/05/2018
Domínio	Privacidade
Classificação	Público
Referência	Apéndice 11A das BCR

Apêndice 11B
Escopo do material das BCR para o Encarregado

Lista de Finalidades do Tratamento e Categorias relacionadas de Dados Pessoais e Titulares dos Dados

Além das disposições da seção 2.1 sobre o escopo material destas BCR-P, a tabela abaixo fornece detalhes adicionais sobre as transferências realizadas sob estas BCR-P. Esta tabela detalha a Finalidade do Tratamento e as categorias relacionadas de Titulares dos Dados e Dados Pessoais cobertos por estas BCR-P. A tabela abaixo fornece detalhes sobre as Transferências de Dados Pessoais realizadas entre as Entidades Membros das BCR enumeradas no Apêndice 1 sob estas BCR-P.

Os países para os quais os dados pessoais podem ser transferidos dependem da localização dos Membros das BCR envolvidos nas atividades de processamento e são fornecidos no Apêndice 1.

Âmbito das atividades de tratamento		Finalidade do tratamento	Categorias de Dados Pessoais	Categorias de Titulares dos Dados
Operação	Atividades relacionadas com centros de contato	**Gestão de Operações de Centros de Contato**	**1. Dados de identificação** (por exemplo, Nome, Sobrenome, E-mail, Número de telefone, Endereço, Código interno de processamento que permite a identificação do Cliente Final) **2. Dados profissionais** (por exemplo, Cargo, função, número de identificação interno do empregado, gerente de linha de reporte) **3. Dados técnicos e de conexão** (por exemplo, Endereço IP, Logins, Dados de ID do dispositivo) **4. Dados de vida pessoal** (do Cliente Final) (por exemplo, Estado civil, número de pessoas no domicílio, número e idade dos filhos no domicílio, ocupação, hábitos de vida e estilo de vida, área de atuação) **5. Dados de gestão de contratos** (por exemplo, Número de transação, detalhes da compra, assinatura, descrição e condições do bem ou serviço adquirido, Histórico da interação entre o Cliente Final e o Controlador do Tratamento) **6. Dados de programas de fidelização e atividades promocionais** (por exemplo, Dados necessários para a gestão e ciclo de programas de fidelização, prospecção, pesquisa, questionários, testes e promoção de produtos)	**Empregados dos Membros das BCR** **Controlador do Tratamento / Cliente Final do Cliente / Prospects** **Empregados e membros do pessoal relacionado do Controlador do Tratamento/Cliente**

Âmbito das atividades de tratamento		Finalidade do tratamento	Categorias de Dados Pessoais	Categorias de Titulares dos Dados
			7. Dados econômicos e financeiros (por exemplo, Informações necessárias para gerenciar a solicitação do cliente final, como Informações sobre pagamentos, condições de pagamento (descontos, abatimentos, etc.), detalhes bancários)	
		Operações de exclusão (durante atividades promocionais)	**1. Dados de identificação** (por exemplo, Nome, Sobrenome, E-mail, Número de telefone, Endereço, Código interno de processamento que permite a identificação do Cliente Final) **2. Dados técnicos e de conexão** (por exemplo, Endereço IP, Logins, Dados de ID do dispositivo) **3. Dados de gestão de contratos** (por exemplo, Informações sobre a decisão do Cliente de cancelar, incluindo por meio de uma lista de "não ligar" de terceiros)	**Empregados dos Membros das BCR** **Controlador do Tratamento / Cliente Final do Cliente / Prospects**

Âmbito das atividades de tratamento		Finalidade do tratamento	Categorias de Dados Pessoais	Categorias de Titulares dos Dados
		Controle de satisfação do cliente final	**1. Dados de identificação** (por exemplo, identificação por meio dos meios utilizados para interagir com o Centro de Contato (número de telefone, número de fax, endereço de e-mail, código interno de processamento que permite a identificação do cliente final)) **2. Dados profissionais** (por exemplo, cargo, função, gerente de linha, localização do escritório) **3. Dados técnicos e de conexão** (por exemplo, endereço IP, logins, dados de identificação do dispositivo) **4. Dados de gestão de contratos** (por exemplo, respostas agregadas fornecidas, resultados da avaliação)	**Empregados dos Membros das BCR** **Controlador do Tratamento / Cliente Final do Cliente / Prospects**
		Prevenção e detecção de fraudes	**1. Dados de identificação** (por exemplo, nome, sobrenome, e-mail, número de telefone, endereço, código interno de processamento que permite a identificação do cliente final) **2. Dados profissionais** (por exemplo, cargo, função, gerente de linha, localização do escritório) **3. Dados técnicos e de conexão** (por exemplo, endereço IP, logins, dados de identificação do dispositivo)	**Empregados dos Membros das BCR** **Controlador do Tratamento / Cliente Final do Cliente / Prospectos** **Empregados do controlador/cliente e pessoal relacionado**

Âmbito das atividades de tratamento		Finalidade do tratamento	Categorias de Dados Pessoais	Categorias de Titulares dos Dados
			4. Dados de interação (por exemplo, informações sobre a solicitação do cliente final, resposta fornecida, transcrição da conversa)	
		Monitoramento, escuta e gravação de interações	**1. Dados de identificação** (por exemplo, nome, sobrenome, e-mail, número de telefone, endereço, código interno de processamento que permite a identificação do cliente final) **2. Dados profissionais** (por exemplo, cargo, função, gerente de linha, localização do escritório, número de identificação interno do empregado) **3. Dados técnicos e de conexão** (por exemplo, endereço IP, logins, dados de identificação do dispositivo) **4. Dados da vida pessoal** (do cliente final) (por exemplo, estado civil, número de pessoas na residência, número e idade dos filhos na residência, ocupação, hábitos de vida e estilo de vida, área de atuação) **5. Dados de gestão de contratos** (por exemplo, número de transação, detalhes da compra, assinatura, descrição e condições do bem ou serviço adquirido), histórico da interação entre o cliente final e o controlador dos dados	**Empregados dos Membros das BCR** **Controlador do Tratamento / Cliente Final do Cliente / Prospectos** **Empregados do controlador/clientes e pessoal relacionado**

Âmbito das atividades de tratamento		Finalidade do tratamento	Categorias de Dados Pessoais	Categorias de Titulares dos Dados
			6 Empleados del responsable/clientes y personal relacionado. Datos de programas de fidelización y actividades externas (por ejemplo, datos necesarios para la gestión y ciclo de programas de fidelización, prospección, investigación, encuestas, pruebas de productos y promoción) **7. Datos económicos y financieros** (por ejemplo, información necesaria para gestionar la solicitud del cliente final, como información sobre pagos, condiciones de pago (descuentos, rebajas, etc.), detalles bancarios) **8. Datos de interacción** (por ejemplo, información sobre la solicitud del cliente final, respuesta proporcionada, transcripción de la conversación)	
		Inteligência empresarial, relatórios e análise	**1. Dados de identificação Dados de identificação** (por exemplo, nome, sobrenome) **2. Dados profissionais** (por exemplo, cargo, função, gerente de linha, localização do escritório) **3. Dados técnicos e de conexão** (por exemplo, endereço IP, logins, dados de identificação do dispositivo) **4. Dados de gestão de contratos** (por exemplo, estatísticas agregadas sobre o cumprimento dos KPIs impostos pelo cliente)	**Empregados dos Membros das BCR** **Controlador do Tratamento / Cliente Final do Cliente / Prospectos** **Empregados do controlador/clientes e pessoal relacionado**

Âmbito das atividades de tratamento		Finalidade do tratamento	Categorias de Dados Pessoais	Categorias de Titulares dos Dados
		Numeração e roteamento de interações / gestão técnica de interações	**1. Dados de identificação** (por exemplo, nome, sobrenome, e-mail, número de telefone, endereço, código interno de processamento que permite a identificação do cliente final) **2. Dados profissionais** (por exemplo, cargo, função, gerente de linha, localização do escritório, número de identificação interno do empregado) **3. Dados técnicos e de conexão** (por exemplo, endereço IP, logins, dados de identificação do dispositivo) **4. Dados de gestão de contratos** (por exemplo, informações sobre a decisão do cliente de cancelar, incluindo através de uma lista de "não ligar" de terceiros)	**Empregados dos Membros das BCR** **Controlador do Tratamento / Cliente Final do Cliente / Prospectos**
		Modificação da voz do agente para moldar sua expressividade e melhorar a comunicação	**1. Dados de identificação** (por exemplo, Nome, Sobrenome, E-mail, Número de telefone, Endereço) **2. Dados profissionais** (por exemplo, cargo, função, gerente de linha de reporte, localização do escritório, número de identificação interno do empregado) **3. Dados técnicos e de conexão** (por exemplo, Endereço IP, Logins, Dados de identificação do dispositivo)	**Empregados dos Membros das BCR**

Âmbito das atividades de tratamento		Finalidade do tratamento	Categorias de Dados Pessoais	Categorias de Titulares dos Dados
	Atividades Netino	**Moderação e interações sociais online**	**1. Dados de** identificação (por exemplo, Nome, Sobrenome, foto do cliente final (se publicada na ferramenta), E-mail, Número de telefone, pseudônimo) **2. Dados técnicos e de conexão** (por exemplo, Endereço IP, Logins, Dados de identificação do dispositivo) **3. Dados de interação** (por exemplo, acesso a dados publicados pelo interessado em uma plataforma)	**Empregados dos Membros das BCR** **Controlador do Tratamento / Cliente Final do Cliente / Prospectos**
	Serviços relacionados com WPS/WKS	**Coleta e Análise de Documentos KYC (em nome dos clientes que solicitam o serviço)**	**1. Dados de identificação** (por exemplo, Nome, Sobrenome) **2. Informações KYC** (por exemplo, decisão de prosseguir/não prosseguir, resultados das investigações KYC)	**Controlador do Tratamento / Cliente Final do Cliente / Prospectos**
		Verificação de antecedentes de solicitantes de clientes / KYE (em nome dos clientes que solicitam o serviço)	**1. Dados de identificação** (por exemplo, Nome, Sobrenome) **2. Informações KYC** (por exemplo, decisão de prosseguir/não prosseguir, resultados das investigações KYC)	**Controlador do Tratamento / Cliente Final do Cliente / Prospectos**

CONTROLE DE DOCUMENTOS

Versão	Atualização	Resumo das modificações
0.1	27/02/2022	Aprovação final
0.2	19/05/2023	Controle de documentos (adicionado) Atualização de países e regiões
0.3	01/04/2024	Rebranding e formato

Frequência de revisão	Este documento será revisado pelo menos uma vez por ano ou sempre que ocorrer uma alteração.
Data de emissão	25/05/2018
Domínio	Privacidade
Classificação	Público
Referência	Apêndice 11B da BCR

Binding corporate rules as controller

Our BCRs **Controller** is applicable only to the Concentrix Affiliate under Webhelp SAS, the latter acting as the European Lead Entity

The Affiliates to which the BCRs apply are listed in Appendix 01 of the BCRs.

concentrix

Content

1. Introduction

Reminder: **Following the Webhelp & Concentrix transaction of September 2023, the commercial name of the group is now Concentrix. However, please note that the scope of the present BCR has not been modified. The BCRs are only applicable to the Affiliates under Webhelp SAS acting as European Lead Entity, Affiliates that are bound by the BCR (Controller and/or Processor) are listed in Appendix 01 and shall be referred as BCR Member.**

At Concentrix Group, we believe that protecting Personal Data is not only a matter of security or compliance with a particular legal framework, but is a matter of individual and organisational commitment. Disclosing and sharing Concentrix standardsthrough , the Binding Corporate Rules for Processors (hereinafter the "BCR-P") and the present Binding Corporate Rules for Controllers (hereinafter the "BCR-C") is of the utmost importance regarding the Data Subjects' legitimate expectations about how their Personal Data is Processed.

In the course of its activities, BCRs Members process both internal and Client Personal Data. In this respect, BCRs Membersprotect the Personal Data it processes on its own behalf by the implementation of appropriate technical, physical and administrative measures and controls, comprised in the present BCR-C. Such controls shall ensure that the whole organisation is Processing Personal Data in a consistent manner, disregarding the nature and/or place of Processing.

This approach is particularly important due to the diversity of activities Concentrix covers on behalf of its Clients.

As a consequence of the above and taking into consideration the requirements introduced by the European Regulation 2016/679 adopted on 27 April 2016 (hereinafter, the "**EU Regulation"** or **"GDPR"**) and standards, regulations and laws applicable in the field of data protection, where they do not contrevene with the EU Regulation, BCR Members will Process Personal Data in accordance with the following principles:

- **Lawfulness** – Personal Data shall be collected and Processed with the Data Subject having given consent to the Processing or when Processing is legitimate or necessary in accordance with Applicable Data Protection Legislation;
- **Fairness** – Personal Data Processing shall take into account the specific circumstances and context in which such Personal Data is Processed;
- **Transparency** – Information and communication relating to the Processing of Personal Data shall be easily accessible, easy to understand, clear and in plain and simple language;
- **Purpose limitation** – Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes;
- **Data minimisation** – Collected Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed;
- **Accuracy** – Personal Data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that Personal Data

that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without undue delay;

- **Storage limitation** – Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed or any other lawful retention;
- **Integrity and confidentiality** – Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical, physical and administrative measures.

Through this BCR-C Concentrix intends to share and specify the detail and the principles applicable to all BCR Members and provide certain group-wide standards allowing the implementation of the BCR-C. Furthermore, Concentrix may make available specific, local or sectorial policies. Should there be a contradiction between this BCR-C and such specific, local or sectorial policies, the terms of the BCR-C shall prevail, unless the contradictory provisions of such specific, local or sectorial policies are more protective of the Data Subject rights and freedom.

As the BCR-C aims at ensuring an adequate and consistent approach throughout the entire Concentrix organisation regarding Personal Data Processing, exceptions which could result from applicable legislations are not reflected in this BCR-C. However, this BCR-C comprises a notification mechanism in section 12.3 where national legislation prevents a BCR Member from complying with the BCR-Cand where specific rules adding to the EU Regulation are provided by EU Member States. As a consequence, local legislation shall be considered as an enforceable exception to this BCR-Cand will be recorded accordingly, following appropriate notification. As specified in section 12.3, where this national legislation imposes a higher level of protection for Personal Data, this national legislation will take precedence over the BCR-C.

2. Scope

2.1 Material scope

This BCR-C is applicable whenever a a BCR Member Processes Personal Data as Data Controller and as a Data Processor for Processing carried out within the Concentrix organization, on behalf of a BCR Member acting as Data Controller.

Due to the diverse range of activities Concentrix covers, Concentrix may have to process various and constantly evolving categories of Personal Data, such as:

Data relating to personal life (e.g. recruitment management, camera recording system, client and prospect lead management) ;

- Economic and financial data (e.g. payroll management, client and prospect lead management,) ;
- Identification data (e.g. suppliers management, non-commercial communication, survey and form, client and prospect lead management) ;
- Technical data (e.g. IT and telephony management, badge management, employee record management) ; or

- Transactional data (e.g. corporate and legal entities management).

The material scope is more precisely detailed in **Appendix 11-A** which provides a detailed table on the Purpose of Processing and the related categories of Data Subjects and Personal data covered by the present BCR-C. **Appendix 01** provides information on the third countries and BCR Members to which Personal Data is transferred.

BCR-C shall apply to all Data Subjects whose Personal Data are transferred within the scope of the BCR-C from a BCR Member under the scope of application of the GDPR. Therefore, the BCR Member acknolewdges that the scope of the BCR-C may, in particular, not be limited to “EEA citizens or EEA residents”.

In addition, this BCR-C applies to the Processing of Personal Data by a BCR Member acting as Data Controller or as Data Processor on behalf of another BCR Member acting as Data Controller, irrespective of the category and nature of such Personal Data.

Furthermore, each BCR Member is also the Data Controller of the Personal Data of its employees as their employer. When Processing Personal Data of ts employees, BCR Members will comply with this BCR-C and will Process Personal Data as described in the Employee Privacy Policy.

2.2 Geographical scope

Concentrix wants to deploy as much as possible a consistent approach within the organization where Personal Data are being Processed. Consequently, all BCR Members, whatever their location or legal jurisdiction, are subject to this BCR-C. Therefore, the present BCR-C shall at least apply to all Personal Data transferred to BCR Members outside the EEA, and onward transfers to other BCR Members outside the EEA. Please be reminded Concentrix entities bound by the present BCR-C (i.e., BCR Members) are listed in Appendix 01.

As a principle, no Transfer of Personal Data shall be carried out by any Concentrix entities unless and until it is bound by this BCR-C to a Concentrix entities not bound by this BCR-C. Any such Transfer cannot be carried out unless this Concentrix affiliate has provided sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing and obligations attached to such Processing will meet the requirements of this BCR-C and ensure the protection of the rights of the Data Subjects.

The BCR Member bound by the BCR-C and the Concentrix entities not bound will enter into a written agreement to guarantee this.

3. Binding nature

3.1 Upon employees of Concentrix

Each BCR Member’s employee, as a Data Subject, shall benefit from the provisions of this BCR-C. As protecting Personal Data is a matter of individual and organisational commitment, each employee must also comply with the requirements specified under this BCR-C.

As such, the BCR-C falls within the set of policies Concentrix employees are required to comply with as part of their employment contract. Failure to comply with the principles and rules of this BCR-C may lead to disciplinary action that could result in the termination of the employment and, in certain circumstances, to criminal charges.

3.2 Upon BCR Members of Concentrix group

As a group, Concentrix wants to ensure that all BCR Members belonging thereto are bound in the same or a similar manner to the principles and obligations specified under this BCR-C and will comply with the requirements specified herein.

For this reason, this BCR-C is binding upon all the BCR Member by signing an Intragroup Data Transfer Agreement comprising this BCR-C as an appendix.

The list of Concentrix entities bound by this BCR-C is set out in Appendix 1 to this BCR-C. Webhelp SAS as Lead European Entity, with the assistance of the DPO, commits to keep this list up-to-date and available and to communicate it on request to the relevant parties as determined from time to time.

3.3 Towards Concentrixes' Data Processors

Where a BCR Member engages a Data Processor (be it a BCR Member, an affiliate of the Concentrix group not yet bound by the BCR or a third party provider) for carrying out specific Processing activities, such Data Processor shall provide sufficient guarantees to implement appropriate technical and organisational measures in a manner that the Processing will meet the requirements of this BCR-C.

Therefore, any Processing activity undertaken by BCR Member's Data Processors shall be governed by a written contract or other binding legal act, and shall set out all elements of article 28 GDPR as reminded below and in particular the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of BCR Member acting as Data Controller.

In addition, this contract or other binding legal act with a Data Processor shall set out the following provisions:

19. The Data Processor shall process the Personal Data only on documented instructions from the Data Controller, including with regards to Personal Data Transfers, uless required to do so by Union or Member State law to which the Data Processor is subject (in such case, the Data Processor shall inform the Data Controller of that legal requirement before processing, unless that law prohibits such informationon important grounds of public interest).
20. The Data Processor shall keep the Personal Data confidential especially by ensuring that persons authorized to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

21. The Data Processor shall take appropriate technical, physical and organizational security measures to ensure an appropriate level of security to protect the Personal Data.
22. The Data Processor shall not permit Sub-Processor to Process Personal Data in connection with its obligation to a BCR Member without the prior written authorization of the BCR Member and shall ensure this Sub-Processor undertakes to comply with the same obligations as provided in the binding act executed between the Data Processor and the BCR Member by way of a contract or other legal act under Union or Member State law. Where the Sub-Processor fails to fulfil its data protection obligations, the initial Data Processor shall remain fully liable to the BCR Member for the performance of that other Data Processor's obligations.
23. The Data Processor shall provide all necessary support to the BCR Member with regards to the handling of requests from Data Subjects relating to their rights.
24. The Data Processor shall provide all reasonable assistance to the BCR Member to:
    - Ensure a level of security of the Processing appropriate to the risk,
    - Without undue delay, inform the BCR Member of any actual or suspected security breach involving Personal Data and support the BCR Member in the notification to the relevant Supervisory Authority and communication to affected Data Subjects as the case may be.
    - Conduct data protection impact assessment (DPIA) and, where relevant obtain prior consultation with the Supervisory Authority where the DPIA result in a high risk in the absence of measures to mitigate the risk.
25. The Data Processor shall comply with the BCR Member's instructions regarding the deletion or return of the personal data at the termination of the contract or other legal binding act, and delete existing copies unless Union or Member State law requires storage of the Personal Data.
26. The Data Processor shall make available to the BCR Member all information necessary to demonstrate its compliance and contribute to audits and inspections by a BCR Member or other relevant authority or auditor mandated by the BCR Member.
27. The Data Processor shall immediately inform the BCR Member if, in its opinion, an instruction infringes this BCR-C or relevant Applicable Data Protection Legislation.

4. Principles for processing personal data

The Applicable Data Protection Legislation defines a set of principles to be observed when Processing Personal Data. Concentrix undertakes to comply with these principles acting as Data Controller or Data Processor on behalf of a BCR Member acting as Data Controller.

4.1 Defining a legal basis for Processing (Transparency, fairness and lawfulness)

When Personal Data is being Processed, it is required that such Processing relies upon an appropriate legal basis as those provided for in article 6 GDPR, such legal basis being the foundation that allows for lawful Processing.BCR Members acknowledge that one of the following legal basis may be applicable fo the Processing of Personal:

- Data Subjects' consent;
- Performance of a contract to which the Data Subject is party or to enter into such contract
- Legal obligation set out under the Union or Member State lawto which the Data Controller is subject
- Vital interest of the Data Subjects or another individual
- Performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller;
- Legitimate interest of the Data Controller or of a third party (provided such interest does not override the rights and freedom of the Data Subjects).
- Or any other

In this respect, BCR Members undertake to lawfully Process Personal Data only where it has a valid legal basis to do so pursuant to the requirements of the Applicable Data Protection Legislation.

For instance, the Processing of Concentrix employees' Personal Data is necessary to manage leave requests (e.g. holidays). Thus, the legal basis for such processing operation is the necessity to execute the employment contract Concentrix and its employees have entered into.

In addition, and in line with Article 5 below BCR Members undertake to ensure that:

- Special Categories of Personal Data may only be processed in line with one the exemptions envisaged by Article 9(2) GDPR apply,, and
- Processing of Personal data relating to criminal convictions and offences shall be prohibited, unless the same exemptions as the ones envisaged by Article 10 GDPR apply.

4.2 Defining a purpose (Purpose limitation)

Unless specifically authorised by Applicable Data Protection Legislation, BCR Members shall ensure that it has ascertained a lawful, fair, explicit and legitimate purpose prior to any collection or Processing of Personal Data.

BCR Members undertake to ensure that the purposes it defines do not breach the Applicable Data Protection Legislation and appear to be legitimate while ensuring Personal Data is not further Processed in a manner that is incompatible with those purposes.

For instance, planning the necessary work force to deliver its services and consequently managing Concentrix employees' schedules is one of the purposes

defined for the collection of Employees' personal data regarding their request for leave.

4.3 Minimizing Personal Data collection (Data minimization)

BCR Members commit to collect and process Personal Data which is strictly adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

Personal Data shall not be collected widely in the perspective of a further undefined purpose.

For instance, Personal Data collected for managing request for leave is limited to the nature of the leave (e.g. holidays, maternity leave etc.) and other relevant information (e.g. duration of the leave), but it does not include any Personal Data which is not strictly necessary (such as with whom the employee is going on holidays, the destination of the employee or any health data for sick leaves).

4.4 Holding a record

Whether acting as a Data Controller or Data Processor, BCR Members shall maintain a record of all categories of Personal Data Processing activities under its responsibility in order to demonstrate compliance with the BCR-C.

Where acting as Data Controller, the Record of Processing Activities should at least mention the following information in line with Article 30.1 of the GDPR:

- The name and contact details of the Concentrix entity, the potential joint controller and the Data Protection Officer;
- The purposes of the Processing;
- The description of the categories of Data Subjects and of Personal Data;
- The categories of recipients of the Personal Data;
- The potential transfers of Personal Data to a third country or an international organisation;
- The Data storage duration;
- A general description of the technical and organisational security measures to ensure a level of security appropriate to the risk of the Processing.

For instance, the Processing operation of managing employees' requests for leave is included in the Record of Processing Activities related to employee administrative management which contains the above listed information.

Where acting as Data Processor, the Record of Processing Activities should at least mention the following information in line with Article 30.2 of the GDPR:

- The name and contact details of the the Processor(s) and of each Controller on behalf of which the processor is acting, and, where applicable, of the Contrllers's or Processor's representative, and the DPO;The categories of Processing carried out on behalf of each Controller;
- Where applicable, Transfers of Personal Data to a third country and, in the appropriate safeguards or exemption applicable in line with Article 49 of the GDPR.

4.5 Accuracy of the Personal Data (Data Accuracy)

BCR Members shall implement adequate measures and controls to ensure that the Personal Data it collects and processes remains accurate and, where necessary, kept up to date. To this end, BCR Members undertake to implement any required actions to take every reasonable step to ensure that Personal Data that is inaccurate, having regard to the purposes for which it is Processed, is erased or rectified.

For instance, Employees have a duty to inform their HR department of any update in their personal situation (e.g. address modification). BCR Members will then ensure the Personal Data will be updated accordingly in the Employees' record.

4.6 Defining a data retention period (Limited storage period)

BCR Members will not keep the Personal Data for a longer period than is strictly necessary having regard to the purpose for which such Personal Data is collected. In this respect, BCR Members commit to determine a data retention period before implementing each Processing.

To ensure compliance with this requirement, BCR Members shall implement a data retention procedure and specify guidelines to be applied with respect to a given Processing activity.

For instance, Personal Data collected for managing leave request are kept as long as necessary to manage the schedules, perform action relating to payroll (e.g. unpaid leave) and to comply with applicable local statute of limitation and accounting obligations.

4.7 Implementing security measures (integrity and confidentiality)

BCR Members have implemented appropriate technical, physical and administrative measures and controls to ensure that Personal Data is not unlawfully accessed and/or Processed. Such technical, physical and administrative measures shall ensure a level of security appropriate to the risk, including, but not limited to, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by any BCR Member and any Data Processor.

In addition, BCR Members ensure that its subcontractors / Processors comply with the technical and organisational security measures implemented at Concentrix by entering into written agreements with them comprising the requirements set out in article 28.3 GDPR (see also Article 3.3 of the BCR-C above).

For instance, BCR Members have elaborated and implemented an Information Security Policy (Appendix 10 to this BCR-C). Locally, BCR Members may have also implemented more specific security policies. When entering into an agreement with subcontractors / Processors, BCR Members reserve themselves the right to

assess the level of security provided by the contracting party to the Processing of Personal Data.

4.8 Data Protection Impact Assessment

The Data Protection Impact Assessment (DPIA) is a risk-based process introduced by the General Data Protection Regulation that enables the Data Controller to describe the Personal Data Processing, to prove its necessity and proportionality and to help manage the risks to the rights and freedoms of natural persons resulting from the Processing of Personal Data by assessing them and determining the measures to address them. BCR Members are committed to conduct DPIAs in accordance with **Appendix 09 Procedure for Data Protection Impact Assessment**.

Where a type of Processing, involving in particular the use of new technologies, is likely to result in a high Risk to the rights and freedoms of Data Subjects, BCR Members shall, taking into account the nature, scope, context and purposes of the processing and prior to the processing, carry out a DPIA. This requirement shall also apply to existing Processing operations where a modification of the processing operation is expected and where such modification may result in a high Risk to the rights and freedoms of Data Subjects.

The processing would require a Data Protection Impact Assessment if two or more of the following is correct:

- The Data processing includes systematic evaluation or scoring of personal aspects relating to natural persons, including profiling and predicting;
- The Data processing is based on automated processing that significantly affects the natural person;
- The Data processing is done on sensitive Data or on Data of highly personal nature;
- The Data is processed on a large scale;
- The processing combines or matches two or more Data processing operations;
- The Data processing includes a systematic monitoring of a publicly accessible area;
- The processing is made on vulnerable persons' or kids' Data;
- The Data processing includes innovative use or application or technological or organisational solutions;
- The Data processing is made for the purposes than those for which the Data were collected;
- The Data processing prevents the Data subjects from exercising their rights or using a service or contract.

In addition, BCR Members shall carry out a DPIA for Processing operations that require a DPIA pursuant to a decision of the relevant EEA Supervisory Authority's list of data processing operations that require a DPIA.

Where a DPIA indicates that the Processing would result in a high Risk in the absence of measures taken by the Controller to mitigate the risk and where a DPIA

reveals high residual Risks, BCR Member will seek prior consultation of the EEA Supervisory Authority before carrying out this Processing.

For instance, managing employees' leave request is not a processing considered to present a high risks to the rights and freedoms of Data Subjects. Although, whenever a BCR Member identifies a processing meeting two or more of the above-listed criteria, a DPIA is conducted under the supervision of the DPO in accordance with the procedure further described in Appendix 9.

4.9 Subprocessing and Transfers outside the Concentrix Group

BCR Members undertake not to Transfer any Personal Data to Data Controllers and/or Data Processors which are not a BCR Member unless such Data Controllers and/or Data Processors provide sufficient guarantees and have implemented appropriate technical and organisational measures, such as the ones provided in the BCR-C, in such a manner that the Processing will meet the requirements of this BCR-C.

In this respect, BCR Members have implemented appropriate technical, physical and administrative measures to ensure and control that Personal Data is not unlawfully accessed and/or Processed.

Any BCR Member is required to enter into a written contract or other binding legal act with any Data Controllers or Data Processors outside the Concentrix Group (or not bound by the BCR-C) if they are Processing Personal Data. The above-mentioned contract or other binding legal act, shall set out the elements mentioned in Article 3.3 . Such contract may include this BCR-C.

Thus, if a BCR Member, acting as Data Controller or Data Processor on behalf of another BCR Member, uses the services of a subcontractor which is established outside the EEA and needs for the Purpose of the services being performed to share its employees' Personal Data (only to the extent necessary for the operations), BCR Member shall assess, prior to the Transfer, that the subcontractor is able to meet the requirements of the BCR-C and secure the Transfer by the appropriate binding legal act.

4.10 Implementing Personal Data Breach notification measures

Where a Personal Data Breach occurs, BCR Members shall comply with the applicable Data Breach procedure adopted by Concentrix.

In any case, BCR Membersshall without undue delay, and where feasible, not later than 72 hours after having become aware of it, notify the Personal Data Breach to (1) Webhelp SAS (as the Liable BCR Member) and the other relevant Local Privacy Leaders when such BCR Memberis acting as a Data Controller , as well as to the

BCR Member acting as a Controller when a BCR Member acting as a processor becomes aware of a Personal Data Breach (2) the competent EEA Supervisory Authority, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The above-mentioned notification shall cover at least the following information:

- Nature of the Personal Data Breach and scope of the Personal Data Breach, including when possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
- Name and contact detail of the (Group) Data Protection Officer ("**DPO**") or other contact point where more information can be obtained
- Describe the consequences likely to result from the Personal Data Breach;
- Describe the measures taken or proposed to be taken by the Data Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Any BCR Member, when Processing Personal Data on its own behalf as a Controller, and when Processing Personal Data on behalf of another BCR Member acting as a Controller , may also need to communicate to the Data Subjects about the Personal Data Breach where such Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons in line with Article 34 of the GDPR. In such circumstances, the communication shall take place without undue delay, and shall cover the above-mentioned elements as the one which would be communicated to the competent EEA Supervisory Authority.

BCR Members shall document any Personal Data Breach and the above mentioned information. Upon request, BCR Members shall make this documentation available to the competent EEA Supervisory Authority.

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, BCR Members will proceed in accordance with the Personal Breach procedure described in **Appendix 08 Procedure for Personal Data Breach Notification**.

5. Processing sensitive data

BCR Members undertake to comply with the provisions of Article 4 – Principles for Processing Personal Data and acknowledges that Sensitive Personal Data requires the implementation of specific protection as such Personal Data could create significant risks in relation to fundamental rights and freedoms of Data Subjects.

BCR Members undertake to process Sensitive Personal Data in accordance with Applicable Data Protection Legislation and where applicable any other sectorial applicable framework adopted by EEA Supervisory Authorities.

Such Processing shall be limited and specific, in particular in relation to Concentrix employees.

Where it intends to process Sensitive Personal Data on its own behalf, BCR Members will ensure that:

- The Processing is necessary and lawful; or

- The Processing is carried out with appropriate safeguards and controls; or
- When necessary, the Data Subject has given explicit consent to the Processing of those Sensitive Personal Data for one or more specified purposes. Such consent shall not be considered as necessary when (1) the Data Subject is not in a position to give his/her consent and the Processing is necessary to protect the vital interests of the Data Subject or of another person; (2) the Data Subject itself has already manifestly rendered the affected Sensitive Personal Data part of the public domain; (3) When applicable, the Processing is explicitly permitted by Applicable Data Protection Legislation or any national law (e.g. registration/protection of minorities); or
- When necessary, the Processing is essential for the purpose of establishing, exercising or defending legal claims, provided that there are no grounds for assuming that the Data Subject has an overriding legitimate interest in ensuring that such data is not Processed.

6. Transfer of Personal Data to third countries and restriction on onward Transfer to non BCR Members

6.1 Transfers and onward Tansfers of Personal Data

In the course of their business, BCRs Members may Transfer Personal Data to other entities of Concentrix group (which are BCR Members or not) or to third parties. Such entities of Concentrix and/or third parties may be located outside the European Economic Area (hereinafter "**EEA**"). In such a case, Transfers of Personal Data are deemed to take place.

Where Personal Data is Transferred, Concentrix will implement specific guarantees in order to ensure that the Personal Data transferred benefit from an adequate level of protection as further detailed below:

- Transfers of Personal Data from a BCR Member, acting as Data Controller to another BCR Member located outside of the EEA and acting either as Data Controller or as Data Processor will be supported by the provisions of this BCR-C; or
- Transfers of Personal Data from a BCR Member acting as Data Controller to either an entity of Concentrix group (which is not a BCR Member) or to third parties which are located outside of the EEA (more, specifically in a non-EEA country that has been granted an adequacy decision by the EU Commission) and that are acting as Data Processor will be supported by a written agreement including the applicable standard contractual clauses adopted by the competent EEA Supervisory Authority and/or the EU Commission, -such as the EU Commission SCCs on Transfers (914/2021), Module 2 Controller to Processor; or;
- Transfers of Personal Data from a BCR Member acting as Data Controller to either an entity of Concentrix (which is not a BCR Member) or to third parties located outside of the EEA, (more, specifically in a non-EEA country that has been granted an adequacy decision by the EU Commission) and that are acting as Data Controller will be supported by a written agreement including the applicable standard contractual

clauses adopted by the competent EEA Supervisory Authority and/or the EU Commission such as the EU Commission SCCs on Transfers (914/2021), Module 1 Controller to Controller).

- In the absence of an adequacy decision or appropriate safeguards as descirived above, Transfers may exceptionally take place if a derogation applies in line with Article 49 GDPR and shall, where relevant be occasional and not repetitive.

In any event, BCR Members commits not to transfer Personal Data to third parties which are not part of the Concentrix group (or to a Concentrix entity which is not a BCR Member) without ensuring first that an adequate level of protection in line with the one provided by the GDPR will be granted to the Personal Data transferred so as to ensure that the level of protection of Data Subjects guaranted under the GDPR is not undermined.

More specifically, BCR Members agree that Personal data that have been transferred under the BCR-C between two BCR Members may only be onward transferred outside the EEA to Data Pocessors and Controllers not bound by the BCR-C provided that the requirements on Transfers set out in Article 44 to 46 of the GDPR and reflected herein are complied with.

6.2 Obligation of the Data Importer in case of government access request

Without prejudice to the obligation of the BCR Member acting as Data Importer to inform the Data Exporter of its inability to comply with the commitments contained in the BCR-C (Article 12.3 below), BCR Member acting as Data Importer will promptly notify the Data Exporter and, where possible, the Data Subject (if necessary with the help of the Data Exporter) if it:

- Receives a legally binding request by a public authority under the laws of the country of destination, or of an another third country, for disclosure of Personal Data transferred pursuant to the BCR-C. Such notification will include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided;
- Becomes aware of any direct access by public authorities to Personal Data transferred pursuant to the BCR-C in accordance with the laws of the country of destination. Such notification will include all information available to the Data Importer.

If prohibited from notifying the Data Exporter and / or the data subject, the Data Importer will use its best efforts to obtain a waiver of such prohibition, with a view to communicate as much information as possible and as soon as possible, and will document its best efforts in order to be able to demonstrate them upon request of the Data Exporter.

The Data Importer will provide the BCR Member acting as Data Exporter, at regular intervals, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.). If the Data Importer is or becomes partially or completely

prohibited from providing the Data Exporter with the aforementioned information, it will, without undue delay, inform the Data Exporter accordingly.

The Data Importer will preserve the above mentioned information for as long as the Personal Data are subject to the safeguards provided by the BCR-C, and shall make it available to the Competent Supervisory Authority upon request.

The Data Importer will review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and will challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law, and principles of international comity.

The Data Importer will, under the same conditions, pursue possibilities of appeal.

When challenging a request, the Data Importer will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the Personal Data requested until required to do so under the applicable procedural rules.

The Data Importer will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the Data Exporter. It will also make it available to the Competent Supervisory Authority upon request.

The Data Importer will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

In any case, Transfers of Personal Data by a BCR Member to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society (see Article 12.3 of the BCR-C in this regards).

7. Rights of Data Subject

7.1 Third Party beneficiary Rights

Whenever a BCR Member Processing Personal Data as Data Controller or as Processor Processing Personal Data on its behalf, **Data Subjects are entitled to enforce this BCR-C as third-party beneficiaries.**

Data Subjects must at least be able to enforce the following elements:

- Legal basis for processing (Article 4.1);
- Purpose limitation of the Processing (Article 4.2);
- Data 16inimization (Article 4.3);
- Limitation of the storage periods (Article 4.6);
- Data accuracy (Article 4.5);
- Security of Personal Data, especially
    - Data protection by design and by default and measures to ensure data security (Articles 12 and 4.7);

    - Personal Data Breach notification where the Personal Data breach is likely to result in a high risk to their rights and freedoms (Article 4.10)
- Specific rules when processing of special categories of Personal Data and Personal Data related to criminal convictions and offences (Article 5);
- Transparency and easy access to this BCR-C; (Article 12.1);
- Onwards transfers (Article 4.9);
- Rights of access, rectification, erasure, restriction, notification regarding rectification or erasure or restriction to each recipient to whom the personal data have been disclosed, objection to processing, right to data portability, right not to be subject to decisions based solely on automated processing, including profiling; (Article 7.4 and 7.5)
- National legislation preventing respect of BCRs (Article 12.3)) and in case of government access requests (Article 6.2);
- Right to complain through the internal complaint mechanism of the companies (Article 8 of the BCRs and Appendix 5 – Article 3.1);
- Cooperation duties with EEA Supervisory Authority (Article 12.4);
- Right to lodge a complaint with the competent EEA Supervisory Authority (choice before the supervisory authority in the Member State of his habitual residence, place of work or place of the alleged infringement) and before the competent court of the EU Member State (choice for the Data Subject to act before the courts where the controller or processor has an establishment or where the Data Subject has his or her habitual residence) (Article 8);
- Duty to inform the Data Subjects about any update of the BCR-C and of the list of BCR Members that are bound by the present BCR-C (Article 13);
- The present Third-party beneficiary rights (Article 7);
- Right to judicial remedies and the right to obtain redress and, where appropriate, compensation in case of any breach of one of the enforceable elements of the BCR-C (Article 7 and 8 of the BCRs, and Appendix 5 – Article 3.4.2);

Thus, BCR Members acknowledge that Data Subjects are entitled to seek judicial remedies and/or remedies before a data protection authority under the conditions defined below, for any non- compliance with one of the enforceable elements of the BCR-C as enumerated above and to receive compensation for any damages resulting from the violation of the BCR-C by any BCR Member.

A BCR Member accepts that Data Subjects may be represented by a not-for-profit body, organisation or association to lodge the complaint on his or her behalf, to exercise the rights enumerated above. Such body, organization or association shall have been properly constituted in accordance with the law of a Member State, have statutory objectives which are in the public interest, and be active in the field of the protection of Data Subjects' rights and freedoms with regard to the protection of their Personal Data.

For the sake of clarity, it is specified that the third party beneficiary rights above described do not extend to those elements of the BCR-C pertaining to internal mechanisms implemented within entities, such as details of training, audit programme, compliance network, and mechanism for updating the BCR-C.

Please note that withouth prejudice to the present Article 7, Concentrix encourages Data Subjects to use the internal complaint mechanism described in Article 8 of the BCRs-C provided below.

7.2 Right to lodge a complaint and obtain judicial remedy, redress and compensation where a BCR Member within the EEA does not comply with the BCR-C

Where a BCR Member within the EEA does not comply with one of the enforceable elements of the BCR-C as enumerated in the previous section 7.1 above, Concentrix acknowledges that the BCR Member within the EEA responsible for the non-compliance, shall bear responsibility and shall take the necessary actions in order to remedy its acts.

.

Concentrix also acknowledges that the Data Subject shall be entitled to:

- lodge a complaint with an EEA Supervisory Authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement; and/or;
- an effective judicial remedy where he or she claims that this BCR-C has been infringed by a BCR Member as Data Controller or by a BCR Member as a Processor Processing Personal Data on its behalf. Concentrix acknowledges that such claim can be brought either before the competent court of the Member State where the BCR Member responsible for the non-compliance is established or before the court where the Data Subject has his or her habitual place of residence.

7.3 Right to lodge a complaint and obtain judicial remedy, redress and compensation where a BCR Member outside of the EEA does not comply with the BCR-C

Where a BCR Member outside of the EEA does not comply with one of the enforceable elements of the BCR-C as enumerated above, Webhelp SAS as European Lead Entity (1) accepts to be the "Liable BCR Member" and as such endorses responsibility for any material and non-material damages resulting from the non-compliance with the BCR-C, including payment of compensation when granted by the competent court, and (2) agrees to take the necessary actions in order to remedy the acts of such other BCR Member outside the EEA.

.

In such circumstances, Webhelp SAS also acknowledges that any Data Subject who considers that the BCR Member located outside the EEA (acting as Data Controller or Data Processor) has breached one of the enforceable elements enumerated in Section 7.1, shall be entitled to:

- lodge a claim with a data protection authority where he/she has his/her place of residence, place of work or where the BCR Member with delegated responsibility is established. And/or;
- an effective judicial remedy as if the violation had been caused by Webhelp SAS instead of the non-EEA located BCR Member, before the courts or judicial authorities where Webhelp SAS is based, or where the Data Subjects has his/her place of residence or place of work

Where Data Subjects can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of the BCR-C, Webhelp SAS will be responsible for demonstrating that such BCR Member outside the EEA was not responsible for the breach of the BCR-C giving rise to those damages, or that no such breach took place. In the event Webhelp SAS can demonstrate that the other BCR Member located outside the EEA was not responsible for the act, then it can also discharge itself from any responsibility.

7.4 Data Subjects Rights

Data Subjects are entitled to benefit from the following rights:

- Have access to the Personal Data relating to him/her and Processed by a BCR Member;
- Request the rectification or deletion of any inaccurate or incomplete Personal Data relating to him/her, and of any Personal Data with respect to which the purpose of Processing is no longer legal or appropriate;
- Request that the Personal Data Processing relating to him/her be limited;
- Object to the Processing of their Personal Data by a BCR Member where such Processing is necessary for the purposes of the legitimate interests pursued by the BCR Member acting as a Data Controller or by a third party, for legitimate interests purposes, including profiling at any time, on grounds relating to their personal individual situation, unless the interets pursued by the BCR Member override the interests rights and freedoms of the Data Subjects;
- Object to the Processing of their Personal Data for marketing purposes, inluding profiling; and
- Receive their Personal Data in a structured, commonly used, machine-readable format and interoperable when the Processing is carried out by automated means

Where a BCR Member is acting as Data Controller, it will handle such request without undue delay and in accordance with the complaint handling procedure specified under Section 8 below.

The BCR Member acting as Data Controller shall communicate any rectification or erasure of Personal Data or restriction of Processing carried out following a Data Subject's request to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort. In addition such BCR Member shall inform the Data Subject about those recipients if the Data Subject requests it.

7.5 Exercising Data Subjects' Rights

Data Subjects are entitled to enforce this BCR-C as third-party beneficiaries, and to exercise their rights with respect to the Processing of their Personal Data by any BCR Member acting as Data Controller. The BCR Member shall ensure that any request or complaint from Data Subject in relation to the exercise of their rights ("**Requests**") is addressed in a timely manner.

Data Subjects can make a request verbally or in writing. BCR Members will provide Data Subjects with accessible means to exercise their rights and, in particular:

1 - A single dedicated contact email to be used irrespective of the country a Data Subject is located in:

dpo@concentrix.com

Local emails can be used in order to take into account local specificities, such as language.

To reach out your local privacy contact, please refer to Appendix 01 - List of Concentrix entities bound by the BCR-C and local Privacy email contacts.

2 - Single portal with Concentrix DPO email address accessible on www.concentrix.com

3 - Single dedicated postal address to be used irrespective of the country a Data Subject is located in:

Group Data Privacy Officer

Legal and Compliance Department

3 rue d'Heliopolis

75017 – PARIS

FRANCE

The DPO, or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the Requests, shall (i) ensure that they have obtained the minimum required information from the concerned Data Subject to address his/her Request (ii), if deemed necessary, obtain as much information as possible to enable the Request to be duly handled.

If there is a doubt about the identity of the individual making the request, mainly when using distance communication means, a BCR Member may be required to ask for more information regarding the Data Subjects. Information collected shall be (i) limited to information that is necessary to confirm who the individual making a request is and (ii) shall not be collected when products or services provided by a BCR Member or its Clients are not delivered under the real identity of the user. Proportionality shall always be assessed by the Data Controller.

In any case, the response to a Data Subject must occur within 1 month at the latest after receiving the Request. Taking into account the complexity and number of the requests, that one-month period may be extended at maximum by two further months, in which case the complainant should be informed accordingly (as detailed in Appendix 5).

Where the Data Subject is not satisfied with the initial response provided by the BCR Member such Data Subject shall be entitled in any case to immediately ask for his or her Request to be re-examined. Data Subject shall provide to the BCR

Member a detailed explanation of the unsatisfactory provisions of the solution previously provided. The BCR Member shall take no longer than 2 months from receipt of the Request for re-examination to determine how it shall be handled and shall inform the Data Subject in writing accordingly.

If a Data Subject Request or complaint is rejected by the BCR Member or the answer does not satisfy the Data Subject or in any case, the Data Subject can contact the DPO and / or can directly lodge a complaint with a competent EEA Supervisory Authority and / or can seek judicial remedy as further detailed above in section 7.1 and 7.2 above.

Further details regarding this Article are available in the following appendix:

- **Appendix 5 - Procedure for Data Subjects' requests where Concentrix acts as Data Controller**

8. Data Subjects complaint handling procedure

Data Subjects are entitled to lodge a complaint directly to a BCR Member regarding the Processing of Personal Data they consider non-compliant with this BCR-C before the BCR Member they deem to be non-compliant. Where the breach is likely to result from an act of a BCR Member located outside the EEA, the Data Subject can lodge the complaint directly before Webhelp SAS as the European Lead Entity.

Data Subjects may raise a complaint by:

(1) Contacting the relevant Local Privacy Leader of the relevant BCR Member by email at the address is provided in Appendix 01 of the BCR-C, and/or

Contacting the Group Data Privacy Officer at dpo@concentrix.com or by mail at 3/5 rue d'Heliopolis, 75017, Paris, France.Such complaint will be handled by the relevant BCR Member(s) in due course and with particular care and attention according to the steps and timing defined herein. Such provisions are also applicable in relation to Data Subjects requests to exercise their rights (see Article 7 above).

In practice, complaints made by Data Subjects will be handled according to the procedure defined under **Appendix 5 - Procedure for Data Subjects' requests where Concentrix acts as Data Controller**.

The BCR Member acting as Data Controller shall provide information on actions taken to the Data Subject / complainant without undue delay, and in any event within one month from the date such complaint is lodged in accordance with the provisions herein. The Complaint shall be handled by a clearly identified department or person with an appropriate level of independence in the exercise of their functions. In practice, the relevant department or person shall be the Legal & Compliance department (more particularly, the relevant Geo Compliance Officer and/or the Local Privacy Leader). Taking into account the complexity and number of the requests, that one-month period may be extended at maximum by two further months, in which case the complainant should be informed accordingly.

In the event the relevant BCR Member decides to reject a complaint made by a Data Subject, such BCR Member undertakes to inform the Data Subject about its

decision and to provide him/her with information regarding the reason for such dismissal.

In the event a BCR Member considers that a complaint made by a Data Subject is justified, such BCR Member commits to implement the corrective measures it deems adequate to remedy such situation as soon as reasonably possible. In addition, the BCR Member will also inform the concerned Data Subject once the corrective measures have been implemented and the situation is remedied.

In any case, BCR Members acknowledge that Data Subjects remain entitled to lodge a claim before an EEA Supervisory Authority and / or to seek judicial remedy. BCR Members further acklowledge that such rights is not dependent on the Data Subjects having used the complaint handling process beforehand, although Data Subjects re encourage to do so.

9. Data protection governance

Concentrix has defined a Data protection organisation and governance which is further defined under Appendix 3.

BCR Members undertake to designate a Data Protection Officer, where required and in line with Article 37 GDPR, or any other person or entity (such as a chief privacy officer) with responsibility to monitor compliance with the BCR-C and enjoying the highest management support for the fulfilling of this task. This organisation is led by the Group Data Privacy Officer who relies on a network of privacy contact points (namely Regional Privacy Leaders, Local Privacy Leaders as well as Business Privacy Referents) and who may be designated as DPO by the relevant BCR Member.

The DPO formally appointed with a Supervisory Authority shall directly report to the highest management level. In addition, the DPO can inform the highest management level if any questions or problems arise during the performance of their duties.

The DPO should not have any tasks that could result in conflict of interests. The DPO should not be in charge of carrying out data protection impact assessments, neither should they be in charge of carrying out the BCR audits if such situations can result in a conflict of interests. However, the DPO can play a very important and useful role in assisting the BCR Members, and the advice of the DPO should be sought for such tasks.

The roles and responsibilities of the network as well as its working governance are further defined under **Appendix 3 – Data Protection organization and governance**

In addition, the DPO can inform the highest management level if any questions or problems arise during the performance of their duties.

The DPO and the Regional and/or Local Privacy Leaders may be contacted at the contact details described in Article 7.5 of the BCR-C and at the local privacy contacts provided in Appendix 01 of the BCR.

10. Training and awareness

Protecting Personal Data is not only a matter of compliance with privacy laws but is part of the embodiment of Concentrix core values. In this context, fostering a privacy culture within the group is essential to make all employees, trainees, and other persons whose conduct in the performance of work is under the direct control of BCR Members accountable for the protection of Personal Data Processed as part of their operations.

Therefore, this BCR-C shall be properly implemented within the whole organisation. To this end, BCR Members have adopted a privacy training program which aims at ensuring that Concentrix employees, trainees, and other persons whose conduct, in the performance of work is under the direct control of BCR Members, are actually aware of the obligations, principles and procedures specified under this BCR-C. In addition to the key GDPR principles and obligations, the training and awareness programme shall cover, among others, procedures for managing requests for access to personal data by public authorities

Such training is aimed at: (i) individuals having permanent or regular access to Personal Data; (ii) individuals involved in the collection of Personal Data; and/or (iii) individuals involved in the development of tools used to process Personal Data.

The training material shall be up-to-date and regularly reviewed, at least annually or upon significant changes in the applicable Data Protection Legislation, in order to ensure it reflects the latest verison of the BCR-C.

The training program will aim at providing:

- A basic level of core knowledge regarding the applicable principles when Processing Personal Data and a good understanding of the existing procedures and their implementation; and,
- Specific training adapted to the different functions within the organisation.

In this regard it is reminded that BCR Members acknowledge no transfer can be made under the BCR-C to another BCR Member, unless the latter is effectively bound by the BCR-C and appropriate training on the BCR-C can effectively be provided to the employees of the respective BCR Member.

BCR Members undertake to ensure that all Concentrix employees, trainees, and other persons whose conduct, in the performance of work is under the direct control of BCR Members, take the training upon arrival and subsequently complete a refresh every year.

Further details regarding this Article are provided in the following appendix:

- **Appendix 04 – Privacy awareness and training program**

11. Privacy by design/privacy by default

In order to ensure that the principles defined under this BCR-C are effectively taken into account and reflected in the different Processing it carries out, Concentrix will take data protection into consideration and implement appropriate technical and organizational measures from the very beginning of any new project.

In order to provide a high level of protection to the Personal Data within the organisation, the principles and obligations defined hereunder will thus be integrated into the design of each project on the basis of privacy by design procedures adopted by Concentrix.

12. Transparency and cooperation

12.1 Communication of the BCR-C

BCR Member commit to ensure that all Data Subjects will be provided with information on their third-party beneficiary rights, with regard to the processing of their Personal Data, and on the means to exercise those rights. Such information is described in Article 7 of the BCR-C.

Concentrix will openly communicate this BCR-C to the Data Subjects and make it easily accessible to any individual. Such communication shall allow any Data Subject to obtain a copy of this BCR-C with no undue delay and in an open format. In addition, a public version of the latest version of the present BCR-C shall be available at any time to Data Subjects on Concentrix website www.concentrix.com. Data Subjects may also request a copy of the BCR-C by contacting the DPO at dpo@concentrix.com.

The public version of the BCRs-C shall at least contain the following information:

- A description of the scope of the BCR-C (Article 2 of the BCR-C),
- The clause relating to the Group's liability (Article 7 of the BCR-C),
- The clauses relating to the data protection principles (Article 4, 4.1, 4.2, 4.3, 4.5, 4.6, 4.7, 4.9 , 4.10 and 5 of the BCR-C),
- The lawfulness of the processing (Articl 4.1 and 5 of the BCR-C),
- Security and personal data breach notifications (Article 4.7 and 4.10 of the BCR-C),
- Restrictions on onward transfers (Article 4.9 and Article 6 of the BCR-C), and
- The clauses relating to the rights of the data subjects (Article 7, 8 and 12 of the BCR-C).

This information should be up-to-date, and presented to Data Subjects in a clear, intelligible, and transparent way. This information should be provided in full, hence a summary hereof will not be sufficient

The public version shall also include all required policies and procedures attached to the BCR-C as an Appendix, especially for BCR-C:

- Appendix 01 - A List of BCR Members bound by the BCR-C and local privacy email contacts
- Appendix 02 Definitions for BCR and Procedures
- Appendix 05 Procedure for Data Subjects' requests where Concentrix acts as Data Controller
- Appendix 11-A BCR-C material scope: List of Purposes of Processing and related Categories of Personal Data and Data Subjects

The other Apppendices are either not applicable to the BCR-C or are internal processes not relevant for Data Subjects to understand and/or exercize their rights.

This above requirements will be met by ensuring that that a simplified public version of the BCR-C containg all information previously listed is available on Concentrix website (www.concentrix.com).

Concentrix will promote the improvement of the privacy and security culture within its organisation by sharing this BCR-C through internal systems and means (e.g., Concentrix Intranet, internal communications, etc.).

12.2 Information to Data Subjects

BCR Members, where acting as Data Controller shall provide Data Subjects any information required by the Applicable Data Protection Legislation. The BCR Member will provide such information without delay and within a reasonable period after obtaining the Personal Data, but at the latest within one month, at the time of first communication or first disclosure with a legitimate recipient. Such information shall be composed at least of the following elements:

- The identity and the contact details of the Data Controller;
- The contact details of the data protection officer (DPO) and/or the Local Privacy Leader;
- The purposes of the Processing and its legal basis;
- If the information is not collected directly from the Data Subject, the categories of Personal Data Processed;
- The recipients of the Personal Data;
- Where applicable, the existence of Data Transfers outside of the EEA, the countries where the Personal Data is transferred to, the measures implemented to ensure an adequate level of protection and the means by which to obtain a copy of them or where they have been made available;
- The data retention period;
- The rights of the Data Subjects as defined under Article 7 above. (e.g. the existence of the right to request from the Data Controller access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or to object to Processing as well as the right to data portability);
- The right to lodge a complaint before a supervisory authority;
- Where Personal Data is collected from the Data Subject, whether the Data Subject (1) is obliged to provide the Personal Data due to any statutory or contractual requirement, or (2) has a requirement to provide the Personal Data as it is necessary to enter into a contract, and of the possible consequences of failure to provide such data;
- If the Processing is based on the consent of the Data Subjects, the right for them to withdraw their consent at any time without affecting the lawfulness of Processing based on consent before its withdrawal;
- If the Processing is based on the BCR Member's legitimate interest, explanations regarding said legitimate interest;
- As the case may be, the existence of automated decision-making, including profiling; and

- Where the Personal Data is not collected from the Data Subject, any available information as to their source (e.g. in particular, categories of Personal Data, source from which the Personal Data originates, public nature of the Personal Data);

BCR Members undertake to provide such information to Data Subjects in accessible, easy to understand, clear and in plain and simple language

12.3 Inconsistencies with local legislations & practices affecting compliance with BCR-C

BCR Members commit to use the BCR-C as a tool for Transfers only where they have assessed that the law and practices in a Non-Adequate third country of destination applicable to the Processing of the Personal Data by the BCR Member acting as Data Importer, including any requirements to disclose Personal Data or measures authorising access by public authorities, do not prevent it from fulfilling its obligations under these BCR-C.

Such commitment is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the below listed purposes are not in contradiction with the BCR-C:

(oo) national security, and/or,
(pp) defence, and/or
(qq) public security, and/or
(rr) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; and/or
(ss) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security; and/or
(tt) the protection of judicial independence and judicial proceedings; and/or
(uu) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; ad/or
(vv) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g); and/or
(ww) the protection of the Data Subject or the rights and freedoms of others; and/or
(xx) the enforcement of civil law claims.

In assessing the laws and practices of the Non-Adequate Third Country which may affect the respect of the commitments contained in the BCR-C, the BCR Members shall take due account, in particular, of the following elements:

- **The specific circumstances of the Transfers** or set of Transfers, and of any envisaged onward Transfers within the same third country or to another Non-Adequate Third country, including:
  - purposes for which the Personal Data are transferred and Processed (e.g. marketing, HR, storage, IT support, clinical trials);
  - types of entities involved in the Processing (the Data Importer and any further recipient of any onward Transfer);
  - economic sector in which the Transfer or set of Transfers occur;
  - categories and format of the Personal Data Transferred;
  - location of the Processing, including storage; and
  - transmission channels used.
- **The laws and practices of the third country of destination** relevant in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorising access by such authorities and those providing for access to these Personal Data during the transit between the country of the Data Exporter and the country of the Data Importer, as well as the applicable limitations and safeguards.
- **Any relevant contractual, technical or organisational safeguards** put in place to supplement the safeguards under the BCR-C, including measures applied during the transmission and to the Processing of the Personal Data in the country of destination.

Where any safeguards in addition to those envisaged under the BCR-C should be put in place, Webhelp SAS, as the Liable BCR Member, the DPO and the relevant Local Privacy Leader will be informed and involved in such assessment.

BCR Members shall document appropriately such assessment, as well as the supplementary measures selected and implemented. Such documentation shall be made available to the competent Supervisory Authority and to the DPO upon request.

In addition, BCR Member acting as Data Importer shall promptly notify the Data Exporter if, when using these BCR-C as a tool for Transfers, and for the duration of the BCR membership, it has reasons to believe that it is or has become subject to laws or practices that would prevent it from fulfilling its obligations under the BCR-C, including following a change in the laws in the Non-Adequate Third Country or a measure (such as a disclosure request). This information should also be provided to the Liable BCR Member and to the DPO.

Upon verification of such notification, the BCR Member acting as Data exporter, along with the Liable BCR Member, and with the assistance of the DPO, the relevant Local Privacy Leader and the Information Security team, should commit to promptly identify supplementary measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the BCR Member acting as Data Exporter and/or Data Importer, in order to enable them to fulfil their obligations under the BCR-C. The same applies if a BCR Member acting as Data Exporter has reasons to believe that a BCR Member acting as its Data Importer can no longer fulfil its obligations under this BCR-C.

Where the BCR Member acting as Data Exporter (along with the Liable BCR Member and the DPO and/or the relevant Local Privacy Leader) assesses that the BCR-C, even if accompanied by supplementary measures, cannot be complied

with for a Transfer or set of Transfers, or if instructed by the competent Supervisory Authority, such BCR Member commits to suspend the Transfer or set of Transfers at stake, as well as all Transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the Transfer is ended.

Following such a suspension, the BCR Member acting as Data Exporter has to end the Transfer or set of Transfers if the BCR-C cannot be complied with and compliance with the BCR is not restored within one month of suspension. In this case, Personal Data that have been transferred prior to the suspension, and any copies thereof, should, at the choice of the BCR Member acting as Data Exporter, be returned to it or destroyed in their entirety.

Webhelp SAS, as the liable BCR Member and the DPO and/or the relevant Local Privacy Leader, will inform all other BCR Members of the assessment carried out and of its results, so that the identified supplementary measures will be applied in case the same type of Transfers is carried out by any other BCR Member or, where effective supplementary measures could not be put in place, the Transfers at stake are suspended or ended.

BCR Member acting as Data Exporters shall monitor, on an ongoing basis, and where appropriate in collaboration with Data Importers, developments in the Non Adequate Third Countries to which the Data Exporters have transferred Personal Data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such Transfers

12.4 Duty to cooperate

In any event, BCR Members agree to cooperate with EEA Supervisory Authorities, including by accepting to be audited or inspected (onsite on remotely) by such Supervisory Authorities, to take into account the advice, and to abide by decision of the competent EEA Supervisory Authority that may be provided in relation to this BCR-C. BCR Members acknowledge and agree that the competent Supervisory Authority powers and audit rights cannot be limited, in particular in relation to the practical audit conducted by such Supervisory Authority.

BCR Members, and where applicable, their respective representative shall make available to the EEA Supervisory Authority, upon request, any information about the processing operations covered by the BCR-C, such as the records of processing activities.

Any dispute related to the competent Superviroy Authority's exercise of supervision of compliance with the BCR-C will be resolved by the courts of the Member State of that Supervisory Authority, in accordance with that Member State's procedural law. The BCR Members agree to submit themselves to the jurisdiction of these courts.

13. Audit programme covering the BCR

Each BCR Member acting as Controller shall be responsible for and able to demonstrate compliance with the BCR-C. To his end, and in addition with the requirements set out in Article 4.4 (Holding a Record), 4.8 (Data Protection Impact Assessment) and Appendices 08 – Personal Data breach Notification, BCR

Members shall comply with the following requirement reagrding data protection audit programme.

BCR Member commit to develop and integrate into its audit program the review of its compliance with this BCR-C. The audit program will enable to define:

- a reasonable frequency according to which audits shall be carried out;
- the expected scope of the audit; and
- the team in charge of the audit.

The audit procedure is detailed in **Appendix 7 – Procedures for Data Privacy Audits**. The audit covers all aspects of this BCR-C (for instance, applications, IT systems, databases that process personal data, or onward transfers, decisions taken as regards mandatory requirements under national laws that conflict with the BCR-C, review of the contractual terms used for the transfers out of the Group to controllers or processors of data, corrective actions, etc.), including methods and action plans ensuring that corrective actions will take place. However, such audit programme does not necessarily need to monitor all aspects of the BCR-C each time a BCR Member is audited, as long as all aspects of the BCR-C are monitored at appropriate regular intervals for that BCR Member.

BCR Members commit to have audits conducted on a regular basis (at least annually and/or if there are indications of non-compliance) to ensure verification of compliance with the BCR-C or considering the risk level of a Processing activity covered by the present BCR-C to the rights and freedoms of Data Subjects.

In addition to the regular audits, specific audits (ad hoc audits) may be requested by the DPO and/or the relevant privacy network member (e.g. the Local Privacy Leader), or any other competent function in Concentrix group such as the internal audit department. Such audits may be conducted by either internal and/or external accredited auditors advised by the DPO and/or the relevant privacy network member. The roadmap is initiated and determined by the DPO and/or the relevant privacy network member, as specified in Appendix 7. In any case, external auditors shall be independent and bound by a confidentiality obligation and/or be under an appropriate statutory obligation of confidentiality.

The DPO is responsible for determining the scope of audits to be performed. To this end, it can consult the Privacy Committee and/or entrust the internal audit team of Concentrix to determine the scope of such audit. The audit may be conducted by the Group DPO and/or the relevant privacy network members (e.g., the Local Privacy Leader) and/or by the internal audit team of the Concentrix group or any other relevant functions within Concentrix provided that:

- the persons in charge are guaranteed independence as to the performance of their duties to these audits; and
- the persons in charge of auditing compliance with the BCR-C, if such situation result in a conflict of interests.

The results of each audit will be submitted to the Group DPO and/or the relevant privacy network members (e.g., Local Privacy Leaders) and/or the Privacy

Committee and/or Webhelp SAS board members for information. The final report, defect identification and remedial actions are to be shared and enforced by the Local Privacy Leader. Based on the Local Privacy Leader assessment, the report may also be shared, where appropriate, to any Business Privacy Referent, local security manager, process / system owners, Concenrix group ultimate parent's board company or the board of the relevant BCR Member subject to the audit or any other required internal employee. Remedial actions will be defined with a prioritisation to determine a schedule for implementing such measures.

Concentrix acknowledges that competent EEA Supervisory Authorities can request communication of the audit results and thus agree to grant them access thereto upon request. The results of the audit reports and relevant internal audit reports will be maintained in a form that the Supervisory Authorities located in the EEA may access them if they utilize their audit right set out below.

BCR Members undertake to ensure that the Competent Supervisory Authorities can have access to the results of the audit upon request and shall not limit such rights, especially on grounds of confidentiality, e.g. related to the protection of business secrets

It is reminded BCR Member shall entitle any competent EEA Supervisory Authority to carry out data protection audits themselves on any issue related to the BCR-C. In this respect, each BCR Member shall permit the EEA Supervisory Authority to audit the relevant BCR Member in order that the EEA Supervisory Authority may obtain the information necessary to demonstrate BCR Member(s) compliance with this BCR-C (see also Article 12.4 above).

14. Change to the BCR-C

Concentrix DPO with the support of the Local Privacy Leaders will ensure that the present BCR-C is kept up to date (for instance to take into account modifications of the regulatory environment, EU data protection authorities recommendations, or changes to the scope of the BCR-C).

In particular, the DPO shall keep up to date a list of entities bound by the BCR-C. Where any new entity of Concentrix becomes effectively bound by the BCR-C (as specified in Article 3.2), the DPO shall update the list and shall inform without undue delay all BCR Members and the relevant EEA Supervisory Authorities via the competent EEA Supervisory Authority.Such updated information will be made available to Data Subjects together with the BCR-C and via the same means.

At least once a year, or when deemed necessary by the DPO, Webhelp SAS will report such changes to the competent EEA Supervisory Authorities. The notification of such changes to EEA Supervisory Authorities will be carried out at least once a year via the competent EEA Supervisory Authority with a brief explanation of the reasons justifying the update. The Supervisory Authorities should also be notified once a year, following the same process, in instances where no changes have been made.

The annual update or notification should also include the renewal of the confirmation regarding the fact that Webhelp SAS, as the Liable BCR Member made appropriate arrangements to enable itself payment of compensation for any

damages resulting from the breach of the BCR-C by BCR Members outside the EEA.

To the same extent where an amendment has substantial impact on the BCR-C or on the level of protection of the rights granted by this BCR-C, Webhelp SAS, with the assistance of the DPO, undertakes to promptly inform BCR Members and EEA Supervisory Authorities.

15. Non-compliance with the BCR-C

By becoming a BCR Member, Data Exporter and Data Importer shall comply with the following requirements:

- No transfer is made to a BCR member unless the BCR member is effectively bound by the BCR-C and can deliver compliance.
- The Data Importer should promptly inform the Data Exporter if it is unable to comply with the BCR-C, for whatever reason, including the situations further described in Article 12.3 of the BCR-C above.
- Where the Data Importer is in breach of the BCR-C or unable to comply with them, the Data Exporter should suspend the Transfer (See also Article 12.3 of the BCR-C above) .

The Data Importer shall, at the choice of the Data Exporter, immediately return or delete the Personal Data that has been Transferred under the BCR-C in its entirety, where:

- The Data Exporter has suspended the transfer, and compliance with this BCR-C is not restored within a reasonable time, and in any event within one month of suspension; or
- The Data Importer is in substantial or persistent breach of the BCR-C; or
- The Data Importer fails to comply with a binding decision of a competent court or Competent SA regarding its obligations under the BCR-C.

The same commitments should apply to any copies of the data. The Data Importer should certify the deletion of the data to the Data Exporter.

Until the data is deleted or returned, the Data Importer should continue to ensure compliance with the BCR-C.

In case of local laws applicable to the Data Importer that prohibit the return or deletion of the transferred Personal Data, the Data Importer should warrant that it will continue to ensure compliance with the BCR-C, and will only process the data to the extent and for as long as required under that local law.

For cases were applicable local laws and/or practices affect compliance with the BCR-C, see Article 12.3 of the BCR-C above.

16. Termination

A BCR Member acting as data importer, which ceases to be bound by the BCR-C may keep, return, or delete the Personal Data received under the BCR-C.

If the Data Exporter and Data Importer agree that the data may be kept by the Data Importer, protection must be maintained in line with Chapter V GDPR and as reflected in Article 6 of the BCR-C.

17. Appendices

- Appendix 01 - List of Concentrix entities bound by the BCR-P and local Privacy email contacts
- Appendix 02 - Definitions for BCRs and Procedures
- Appendix 03 - Privacy Governance and organization
- Appendix 04 - Privacy awareness and training program
- Appendix 05 - Procedure for Data Subjects' requests where BCR Members acts as Data Controller
- Appendix 06 - Procedure for Data Subjects' requests where BCR Members acts as Data Processor
- Appendix 07 - Audit Procedure
- Appendix 08 - Personal Data Breach Procedure
- Appendix 09 - Data Protection Impact Assessment
- Appendix 10 - Informaiton Security Policy
- Appendix 11-A BCR-C List of Purposes of Processing and related Categories of Personal Data and Data Subjects (Material Scope)
- Appendix 11-B BCR-P List of Purposes of Processing and related Categories of Personal Data and Data Subjects (Material Scope)

DOCUMENT CONTROL

Version	Update	Modification summary
0.1	27/02/2022	Final approval
0.2	01/01/2023	Update of list of BCR Members
0.3	24/02/2023	Update of list of BCR Members
0.4	01/04/2024	Re-branding and formatting Alignment with EDPB Recommendations 1/2022 repealing and replacing WP256_Rev01

Review Frequency	This document will be reviewed at least annually or upon change in Webhelp entities
Date of Issue	25/05/2018
Domain	Privacy
Classification	Public
Reference	EN__GPPriv-01- Binding Corporate Rules - Controller

17.1
17.2
17.3
17.4

17.5
17.6 Appendix 01

List of Concentrix entities bound by the BCR and local privacy email contacts

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
170.	Webhelp Albania Shpk	Rruga Dervish Hima, Stadiumi Air Albania, Qendra e Biznesit, Shkalla BC, nr.B-C, Niveli +3, 1019 Tirana	Albania	privacy@it.webhelp.com
171.	Webhelp Algerie SPA	16bis, cité Bois des Cars 2 16047 Dely Ibrahim	Algeria	privacy@dz.webhelp.com
172.	Webhelp Australia Pty Ltd	Level 16, 201 Elizabeth Street Sydney NSW 2000	Australia	privacy@my.webhelp.com
173.	Webhelp Austria GmbH	Floridsdorfer Haptstrasse 1, 1210 Vienna	Austria	privacy@de.webhelp.com
174.	Webhelp Payment Services Benelux, SA	Avenue Louise, 87 - 1050 Bruxelles	Belgium	privacy@wps.webhelp.com
175.	Webhelp Benin	Immeuble le Jatoba, avenue Jean-Paul II, lot 20, zone résidentielle portuaire; (Nouveau site en cours : Parcelle F G Ilot 40002,quartier Enagnon Akpakpa Cotonou)	Bénin	Privacy@fr.webhelp.com
176.	Webhelp BH d.o.o. Sarajevo	Josipa Stadlera 6, 71000, Sarajevo	Bosnia-Herzegovina	privacy@de.webhelp.com
177.	Services Tech Experience Inovaçao	Rua Marechal Deodoro, 314	Brazil	protecciondedatos@onelinkbpo.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
	e technologia em relacionamento Ltda	6th Floor, Sets 601-606, Centro Curitiba, Paraná, 80.010-010		
178.	Services Assessoria Digital Ltda	Rua Marechal Deodoro 314, 11th floor,Centro Curitiba, Paraná, 80.010-010	Brazil	protecciondedatos@onelinkbpo.com
179.	Webhelp Bulgaria EOOD	Blvd. Totleben, Business-Center Sofia City-West 53-55, 1606, Sofia	Bulgaria	privacy@de.webhelp.com
180.	Les services Webhelp, Inc	880 Rue Roy Est, QC H2L 1E6, Montréal, Quebec	Canada	protecciondedatos@onelinkbpo.com
181.	Webhelp Business Consulting (Shanghai) Co. Ltd	Room 368, Unit 302, No. 211, North Fude Road, Shanghai FTZ	China	privacy@my.webhelp.com
182.	Webhelp (Suzhou) Data Services Co. Ltd	Unit 2605B, 26th Floor, West Tower, China Overseas Fortune Center, No. 9 Suzhou Avenue West, Suzhou Industrial Park	China	privacy@my.webhelp.com
183.	Onelink SAS	Carrera 52 No. 65 91 OF 740 CENTRO COMERCIAL AVENTUR, Medellín	Colombia	protecciondedatos@onelinkbpo.com
184.	Onelink International SAS	Avenida carrera 19 # 28 80 Cc Empresarial Calima Of 401, Bogota	Colombia	protecciondedatos@onelinkbpo.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
185.	Experts Colombia SAS	Carrera 52 No. 65 61, Medellín	Colombia	protecciondedatos@onelinkbpo.com
186.	Getcom Colombia SAS	Diagonal 55 No. 37 41 OF. 601	Colombia	protecciondedatos@onelinkbpo.com
187.	Getcom Servicios SAS	Diagonal 55 Av 37 41 OF 701, Bello	Colombia	protecciondedatos@onelinkbpo.com
188.	Webhelp Enterprise Sales Solutions, s.r.o	Vaclavske namesti 808/66, 11000 Praha, Nové Mesto	Czech Republic	privay@cz.webhelp.com
189.	Webhelp Denmark, AS	Borgmester Christiansens Gade 50, 2, 2500, Copenhagen	Denmark	privacy@nordic.webhelp.com
190.	Webhelp Egypt	plot No. 53, First District, City Center New Cairo, Cairo	Egypt	privacy@eg.webhelp.com
191.	Onelink SA de CV	Avenida Albert Einstein y Bulevar, San Salvador.	El Salvador	protecciondedatos@onelinkbpo.com
192.	Tetel SA de CV	Avenida Albert Einstein y Bulevar, San Salvador.	El Salvador	protecciondedatos@onelinkbpo.com
193.	Getcom International SA de CV	Boulevard Los Próceres, Colonia Palermo Edificio Ex Panades, No. 350, Frente a UCA, San Salvador, San Salvador.	El Salvador	protecciondedatos@onelinkbpo.com
194.	RH-T SA de CV	Avenida Albert Einstein y Bulevar, San Salvador.	El Salvador	protecciondedatos@onelinkbpo.com
195.	Webhelp OÜ	Tartu mnt 63, Tallinn 10115	Estonia	privacy@nordic.webhelp.com
196.	Webhelp Finland, Oy	Palkkatilanportti 1	Finland	privacy@nordic.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
		FI-0240 Helsinki		
197.	GoBeyond Partners, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell , 75017 Paris	France	Privacy@fr.webhelp.com
198.	Webhelp, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	Privacy@fr.webhelp.com
199.	Webhelp Conseil, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	Privacy@fr.webhelp.com
200.	W Automobile Services, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell	France	Privacy@fr.webhelp.com
201.	Webhelp France, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	Privacy@fr.webhelp.com
202.	Webhelp Caen, SAS	1 rue Jean Perrin, 14460 Colombelles	France	Privacy@fr.webhelp.com
203.	Webhelp Compiègne, SAS	ZAC du Parc Tertiaire - 98 impasse Les Terres auprès des Iles, 60610, Compiègne	France	Privacy@fr.webhelp.com
204.	Webhelp Fontenay, SAS	6 Rue de l'Innovation, 85200 Fontenay-le-Comte	France	Privacy@fr.webhelp.com
205.	Marnix French ParentCO, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@webhelp.com
206.	Marnix French TOPCO, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
207.	Marnix, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@webhelp.com
208.	WowHoldCo, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@webhelp.com
209.	Webhelp Gray, SAS	ZAC GRAY SUD 70100 GRAY	France	privacy@fr.webhelp.com
210.	Webhelp Montceau, SAS	16 rue Saint-Eloi, 71300, Montceau les Mines	France	privacy@fr.webhelp.com
211.	Webhelp Vitré, SAS	Parc d'Activité Etrelles, 35370 Etrelles	France	privacy@fr.webhelp.com
212.	Webhelp University France, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@fr.webhelp.com
213.	Webhelp Prestations, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@fr.webhelp.com
214.	Webhelp WTG, SAS	39 rue des métissages 59200 Tourcoing	France	privacy@fr.webhelp.com
215.	Webhelp Medica Customer Expérience	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@webhelpmedica.com ; privacy@patientys.webhelp.com
216.	Patientys, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@webhelpmedica.com ; privacy@patientys.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
217.	MED-TO-MED, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@webhelpmedica.com ; privacy@patientys.webhelp.com
218.	WGE (Webhelp Grand-Est, SAS)	Technopole, 9 rue Thomas Edison, Metz	France	privacy@fr.webhelp.com
219.	Webhelp Medica, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@webhelpmedica.com ; privacy@patientys.webhelp.com
220.	Webhelp SFIA, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@fr.webhelp.com
221.	Webhelp WCS, SAS	12 Rue Alfred Kastler 71530 Fragnes-La Loyere	France	privacy@fr.webhelp.com
222.	Netino, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy@fr.webhelp.com
223.	Solvencia, SAS	450 Rue Félix Esclangon, 73290 La Motte-Servolex	France	privacy@wps.webhelp.com
224.	Webhelp O2C Holding, SAS	450 Rue Félix Esclangon, 73290 La Motte-Servolex	France	privacy@wps.webhelp.com
225.	Webhelp KYC Services, SAS	450 Rue Félix Esclangon, 73290 La Motte-Servolex	France	privacy@wps.webhelp.com
226.	Webhelp Payment Services France, SAS	450 Rue Félix Esclangon, 73290 La Motte-Servolex	France	privacy@wps.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
227.	Webhelp Payment Services Deutschland, GmbH	Frankfurter Str. 151A, 63303 Dreieich	Germany	privacy@wps.webhelp.com
228.	Webhelp Sun Holding GmbH	Tullnaustrasse 20, 90402, Nuremberg	Germany	privacy@de.webhelp.com
229.	Webhelp Holding Germany GmbH	Tullnaustrasse 20, 90402 Nuremberg	Germany	privacy@de.webhelp.com
230.	Webhelp Deutschland GmbH	Tullnaustrasse 20, 90402 Nuremberg	Germany	privacy@de.webhelp.com
231.	RIGHTHEAD GmbH	Tullnaustrasse 20, 90402 Nuremberg	Germany	privacy@de.webhelp.com
232.	Webhelp Ghana Ltd	SU TOWER, N°18, Castle Road, North Ridge, Accra	Ghana	privacy@fr.webhelp.com
233.	Webhelp Hellas Business Enterprise Sales SMLTD (MEPE in Greek)	36 Voukourestiou Str 10673 Athens	Greece	privacy@gr.webhelp.com
234.	Onelink Guatemala SA	15 Avenida 17-30 Zona 13, Oficina 201, Guatemala, Guatemala	Guatemala	protecciondedatos@onelinkbpo.com
235.	Onelink Solutions Guatemala SA	15 Avenida 17-40 zona 13, Torre 1, Nivel 1 Edificio Tetra Center, Ciudad de Guatemala	Guatemala	protecciondedatos@onelinkbpo.com
236.	Inversiones Xperts Guatemala SA	15 Avenida 17-40 zona 13, Torre 1, Nivel 1 Edificio	Guatemala	protecciondedatos@onelinkbpo.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
		Tetra Center, Ciudad de Guatemala		
237.	Gobeyond Partners Asia Limited	31/F Tower Two Times Square 1, Matheson St., Causeway Bay, Hong Kong	Hong Kong	privacy@my.webhelp.com
238.	Webhelp India Private Ltd	Corporate Office: Ground Floor, Tower A, SP Infocity, Udyog Vihar, Phase-1, Gurugram-122001, Haryana , India	India	privacy@uk.webhelp.com
239.	SELLBYTEL Marketing Services India Private Ltd	Corporate Office:- Ground Floor, Tower A, SP Infocity, Udyog Vihar, Phase-1, Gurugram-122001, Haryana , India	India	privacy@uk.webhelp.com
240.	Webhelp Israel Ltd	Yigal Alon 94, Alon tower 1 Tel Aviv , Tel-Aviv	Israel	privacy@tr.webhelp.com
241.	Webhelp Payment Services Italia, SRL	Via Gozzano Guido 14 - 20092 Cinisello Balsamo	Italy	privacy@wps.webhelp.com
242.	Webhelp Payment Services France succursale Italie	Via Maurizio Gonzaga n° 7	Italy	privacy@wps.webhelp.com
243.	Webhelp Enterprise Sales Solutions Italy	Via Torri Bianche, 7, 20871 Vimercate MB, Italy	Italy	privacy@it.webhelp.com
244.	Webhelp Cote d'Ivoire	Immeuble PIA, Avenue Abdoulay Fadiga,	Ivory Coast	privacy@ci.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
		Plateau Abidjan - 01 BP 7171 ABJ 01		
245.	WH Abidjan Le Workshop	Indenie, 6 rue des Sambas 01 BP 743 ABJ 01, Plateau Abidjan - 01 BP 743 ABJ 01	Ivory Coast	privacy@ci.webhelp.com
246.	Webhelp SAS (succursale Côte d'Ivoire)	Immeuble PIA, Avenue Abdoulay Fadiga, Plateau Abidjan - 01 BP 7171 ABJ 01	Ivory Coast	privacy@ci.webhelp.com
247.	Webhelp Japan KK	Tokyo Club Building 11F, 3-2-6 Kasumigaseki, Chiyoda-ku, Tokyo	Japan	privacy@my.webhelp.com
248.	Webhelp Jordan LLC	Rafiq Al Hariri Ave 1, Amman	Jordan	privacy@jo.webhelp.com
249.	IQ-to-Link shpk	Rr. Ukshin Hoti nr. 121	Kosovo	privacy@de.webhelp.com
250.	Webhelp Kosovo L.L.C.	Rr. Ukshin Hoti nr. 120, 10000, Prishtina	Kosovo	privacy@de.webhelp.com
251.	Webhelp Latvia SIA	Krišjāņa Valdemāra iela 21-18	Latvia	privacy@jo.webhelp.com
252.	Webhelp SIA	Skanstes iela 54A	Latvia	privacy@de.webhelp.com
253.	Webhelp Madagascar, SA (zone franche)	Bâtiment TITAN 2, Zone Galaxy Andraharo, Antananarivo 101	Madagascar	privacy@mg.webhelp.com
254.	Netino Madagascar	Lot II M92 Antsakaviro - Ambodirotra Cua	Madagascar	privacy@mg.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
		Antananarivo 101 Analamanga		
255.	Webhelp Malaysia Sdn Bhd	Menara Exchange 106, Level 6, Lingkaran TRX, Jalan Tun Razak, 55188 Kuala Lumpur, Malaysia	Malaysia	privacy@my.webhelp.com
256.	Onelink Mexico SA de CV	BOULEVARD 300 ENTRE CALLE CDA MEZTISOS - VILLAS DEL REY - CAJEME-OBREGÓN SONORA-MÉXICO, 85136, Ciudad Obregón	Mexico	protecciondedatos@onelinkbpo.com
257.	Onelink Servicios SA de CV	BOULEVARD 300 ENTRE CALLE CDA MEZTISOS - VILLAS DEL REY - CAJEME-OBREGÓN SONORA-MÉXICO, 85136, Ciudad Obregón	Mexico	protecciondedatos@onelinkbpo.com
258.	Webhelp Maroc, SA	43 av Ibn Sina-Agdal-Rabat	Morocco	privacy@ma.webhelp.com
259.	Webhelp SAS Succursale	28 Avenue Allal Ben Abdellah - (Business address: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy@ma.webhelp.com
260.	Webhelp Services, SA	15, Avenue Annakhil (Business address: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy@ma.webhelp.com
261.	Webhelp Contact Center, SA	N°50 BLOC F 11 IMMEUBLE AL FIDIAN I ET IMMEUBLE AL	Morocco	privacy@ma.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
		FIDIAN II AVENUE HASSAN I CITE DAKHLA (Business address: 43 av Ibn Sina-Agdal-Rabat)		
262.	Webhelp Multimedia, SA	6, rue Lalla Nezha, 30000 Fès	Morocco	privacy@ma.webhelp.com
263.	Webhelp GRC, SA	43 Avenue Ibn Sina, 10000 Rabat	Morocco	privacy@ma.webhelp.com
264.	Webhelp Technopolis, SA	Agdal, 25, Rue Oued Al Makhazine (Business adress: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy@ma.webhelp.com
265.	Webhelp University Maroc, SARL	15 av Annakhil, (Business adress: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy@ma.webhelp.com
266.	Webhelp Agadir, SA	Quartier Industriel, Avenue Hassan II, Immeuble Jaouhara (Business adress: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy@ma.webhelp.com
267.	Webhelp Fès, SA	112 Avenue des FAR Champs de Course ville nouvelle (Business adress: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy@ma.webhelp.com
268.	Webhelp Meknès, SA	Immeuble Angle Rue Badir Al Kobra et Rue Sebou angle rue Badr al Korba, Meknes	Morocco	privacy@ma.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
		(Business adress: 43 av Ibn Sina-Agdal-Rabat)		
269.	Webhelp Marrakech, SA	Quartier Industriel, Avenue Hassan II, Immeuble Jaouhara (Business adress: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy@ma.webhelp.com
270.	Webhelp Afrique	CFC Bridge, lot 58, Rez de Chaussée (Core 1), quartier Casa-Anfa, Hay Hassani - Casablanca	Morocco	privacy@ma.webhelp.com
271.	Webhelp Netherlands Holding, BV	Amersfoortsestraat 28, 3821CB, Amersfoort	Netherlands	privacy@nl.webhelp.com
272.	Customer Contact Management Group, BV	Amersfoortsestraat 28, 3821CB, Amersfoort	Netherlands	privacy@nl.webhelp.com
273.	Webhelp Nederland, BV	Koraalrood 50, 2718SC Zoetermeer	Netherlands	privacy@nl.webhelp.com
274.	Webhelp Enterprise BV	Brammelerstraat 8, 7511JG Enschede	Netherlands	privacy@nl.webhelp.com
275.	Stacelet Holding, BV	Colosseum 42, 7521 PT Enschede	Netherlands	privacy@nl.webhelp.com
276.	Telecats BV	Colosseum 42, 7521 PT Enschede	Netherlands	privacy@nl.webhelp.com
277.	Customer Contact Performance Group B.V.	Herengracht 501 H, 1017B, Amsterdam	Netherlands	privacy@nl.webhelp.com
278.	CCPG Amsterdam B.V.	Herengracht 501 H, 1017B, Amsterdam	Netherlands	privacy@nl.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
279.	CCPG Utrecht B.V.	Herengracht 501 H, 1017B, Amsterdam	Netherlands	privacy@nl.webhelp.com
280.	Xperts Nicaragua SA	Plaza El Sol 2 C. Sur, 1 C. Este, Casa No. 26, Los Robles Managua	Nicaragua	protecciondedatos@onelinkbpo.com
281.	Onelink Nicaragua SA	Barrio Largaespada. B. Largaespada Busto Jose Marti 3 C al Este 1 C al Norte, Managua	Nicaragua	protecciondedatos@onelinkbpo.com
282.	Webhelp Company Severna Makedonija DOOEL Skopje	Bul. VMRO 1, 1000, Skopje, North-Macedonia	North-Macedonia	privacy@de.webhelp.com
283.	Webhelp Norway, AS	Storgata 38, 0182 Oslo	Norway	privacy@nordic.webhelp.com
284.	Webhelp Norway Consulting AS	Storgata 38, 0182 Oslo	Norway	**privacy@nordic.webhelp.com**
285.	Webhelp Perù S.A.C.	Calle Santa Inés Nro. 115, Urbanización Industrial Santa Rosa, distrito Ate, Lima	Peru	protecciondedatos@onelinkbpo.com
286.	BPO Consulting S.A.C.	Jirón Marcos Farfán, n° 3468, Lima	Peru	protecciondedatos@onelinkbpo.com
287.	Webhelp Philippines, Inc.	12th floor, Makati Sky Plaza, 7788 Ayala avenue, Makati City, 1223	Philippines	privacy@my.webhelp.com
288.	Webhelp Poland Sp. z.o.o.	Ul. Taneczna 30, PL 02-829, Warszawa	Poland	privacy@de.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
289.	Webhelp Sun Portugal, Unipessoal, Lda	Avenida Professor Cavaco Silva, Tagus Park, Edificio Qualidade, bloco A-2, 2470-296 Porto Salvo, parish of Porto Salvo, Oeiras	Portugal	privacy@pt.webhelp.com
290.	Webhelp Oeiras, Lda	Avenida Professor Cavaco Silva, Tagus Park, Edificio Qualidade, bloco A-2, Lisboa	Portugal	privacy@pt.webhelp.com
291.	Webhelp Lisbon, Unipessoal, Lda	Avenida D. João II, nº 43, Torre Fernão de Magalhães, 15º Piso, freguesia de Parque das Nações, 1998-025, Lisboa	Portugal	privacy@pt.webhelp.com
292.	Webhelp SAS Succursale em Portugal	Avenida D. João II, nº 43, Torre Fernão de Magalhães, 15º Piso, freguesia de Parque das Nações, 1998-025 Lisboa	Portugal	privacy@pt.webhelp.com
293.	Webhelp Norte, Unipessoal LDA	Av. Mediterrâneo 1, 1990-203 Lisboa, freguesia de Parque das Nações, LIsboa	Portugal	privacy@pt.webhelp.com
294.	Righthead - Empresa de Trabalho Lda	Avenida Professor Cavaco Silva, Tagus Park, Edificio Qualidade, bloco A-2	Portugal	privacy@pt.webhelp.com
295.	WH New Generation Lisbon	Av. Mediterrâneo 1, 1990-203 Lisboa, freguesia de Parque das Nações, 1998-025, Lisboa	Portugal	privacy@pt.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
296.	Webhelp SFIA, Sucursal em Portugal	Av. Mediterrâneo 1, 1990-203 Lisboa, freguesia de Parque das Nações, 1998-025, Lisboa	Portugal	privacy@pt.webhelp.com
297.	Webhelp Payment Services Espana, Sucursal em Portugal	Av. Mediterrâneo 1, 1990-203 Lisboa, freguesia de Parque das Nações, 1998-025, Lisboa	Portugal	privacy@wps.webhelp.com
298.	Webhelp Romania SRL	Sector 1, Str. Doctor Iacob Felix, nr. 63-69, et. 2	Romania	privacy@ro.webhelp.com
299.	Pitech Plus SA	Strada Câmpul Pâinii nr.3-5, etajul 3	Romania	privacy@ro.webhelp.com
300.	MindMagnet Plus SRL	Strada Câmpul Pâinii nr.3-5, etajul 3, 400058, Cluj-Napoca	Romania	privacy@ro.webhelp.com
301.	Webhelp Senegal SAS	Almadies, Pointe des Almadies, en face King Fahd, fahd Palace, 284, TF n°284/NGA Dakar	Senegal	privacy@sn.webhelp.com
302.	Webhelp SAS Succursale Senegal	Almadies, Imm Serenity Pointe des Almadies, en face King Fahd, fahd Palace TF n°284/NGA Dakar	Senegal	privacy@sn.webhelp.com
303.	Webhelp d.o.o Beograd	Makedonska 30, III. Floor, 11000, Beograd	Serbia	privacy@de.webhelp.com
304.	Webhelp Singapore Pte Ltd	9 Raffles Place, #26-01 Republic Plaza, Singapore 048619	Singapore	privacy@my.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
305.	Webhelp Slovakia, s.r.o.	Staromestská 3 811 03, Bratislava - mestská časť Staré Mesto	Slovakia Republic	privacy@it.webhelp.com
306.	Webhelp Holding Germany GmbH (Slovenia Branch)	City Centre - Republic square, 1000, Ljubljana	Slovenia	privacy@de.webhelp.com
307.	Concentrix South Africa (Pty) Pty Ltd	19 Ameshoff Street, Braamfontein, Johannesburg, 2001	South-Africa	privacy@uk.webhelp.com
308.	Webhelp SAS, Sucursal en Espana	Plaza Solymar s/n, Edificio Benalmar ,29630 Benalmádena, Málaga	Spain	**privacy@es.webhelp.com**
309.	Direct Medica Iberica S.L.	CL LAGASCA, 95, 28006 MADRID	Spain	privacy@webhelpmedica.com
310.	Webhelp Malaga SLU	Plaza Solymar s/n Edificio WEBHELP, 29630 Benalmádena, Málaga	Spain	privacy@es.webhelp.com
311.	Webhelp Payment Services Espana SA	Calle Vallespir, número 19, módulo 3, planta 1ª de Sant Cugat del Vallès	Spain	privacy@wps.webhelp.fr
312.	Webhelp Spain Business Process Outsourcing S.L.	Avda. Diagonal 197 Barcelona, 08018	Spain	privacy@es.webhelp.com
313.	Webhelp Spain Holding SLU	Av. Diagonal 97, 12 Barcelona 08018	Spain	privacy@es.webhelp.com
314.	Telenamic NV	Zonnebloemstraat 50, Paramaribo	Suriname	privacy@sr.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
315.	Webhelp Sweden AB	Box 4006, 16904 Solna	Sweden	
316.	Webhelp IT Services AB	Box 4006, 16904 Solna	Sweden	privacy@nordic.webhelp.com
317.	Webhelp Schweiz AG	Richtistrasse 5, 8304 Wallisellen	Switzerland	privacy@de.webhelp.com
318.	Webhelp (Thailand) Limited	87/1 Capital Tower All Seasons Place, Unit 1604-6 Floor 16, Pathumwan District, 10330, Bangkok	Thailand	privacy@my.webhelp.com
319.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş. (Webhelp Call Center and Customer Service Joint Stock Company).	Merkez Mh. Ayazma Cd. Papirus Plaza No.37/42	Turkey	privacy@tr.webhelp.com
320.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş. Bingöl Branch (Webhelp Call Center and Customer Service Joint Stock Company).	Bingöl Üniversitesi Fen Edebiyat Fakültesi No:Merkezi Derslik Birimi Bodrum Kat:1 Merkez/Bingöl, 12000 Bingöl	Turkey	privacy@tr.webhelp.com
321.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş.İzmir 2 Branch (Webhelp Call Center and Customer Service Joint Stock Company).	Beyazevler Mahallesi Akçay Cad. No: 99/2, 35410 Gaziemir/ Izmir	Turkey	privacy@tr.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
322.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş.Van 2 Branch (Webhelp Call Center and Customer Service Joint Stock Company).	Vali Mithat Bey Mahallesi Cemaller Sk. Roza Aprt Sit. No: 9 A ipekyolu/65100 Van,	Turkey	privacy@tr.webhelp.com
323.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş.Ümraniye Branch (Webhelp Call Center and Customer Service Joint Stock Company).	Fatih Sultan Mehmet Mahallesi Balkan Cad. Casper Plaza İş Merkezi Apt. No: 47/1 Ümraniye / 34771 Istanbul	Turkey	privacy@tr.webhelp.com
324.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş.Bursa Branch (Webhelp Call Center and Customer Service Joint Stock Company).	Panayır Mahallesi 3. Pınar Cad. No:345 B Osmangazi/ 16250 Bursa	Turkey	privacy@tr.webhelp.com
325.	Bin Çağrı Hizmetleri A.Ş. (Bin Call Services Joint Stock Company)	Bingöl Üniversitesi Fen Edebiyat Fakültesi - Bingöl	Turkey	privacy@tr.webhelp.com
326.	Webhelp İnsan Kaynkaları Danışmanlık ve Destek Hizmetleri A.Ş. (Webhelp Human Resources Consultancy and Support Services	Merkez Mh. Ayazma Cd. Papirus Plaza No.37/42, 34406; Kağıthane - Istanbul	Turkey	privacy@tr.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
	Joint Stock Company)			
327.	Teknofix Telekomünikasyon ve Bilişim Hizmetleri A.Ş. (Teknofix Telecomunication and Information Services Joint Stock Company)	Aydınevler Mah. Aslanbey Cad. No:1 D:5-6, Küçükyalı, Maltepe, Istanbul	Turkey	privacy@tr.webhelp.com
328.	Teknofix Telekomünikasyon ve Bilişim Hizmetleri A.Ş. Istanbul Kagithane Branch (Teknofix Telecomunication and Information Services Joint Stock Company)	Merkez Mh. Ayazma Cd. Papirus Plaza No.37/42, 3440 Kağıthane - Istanbul	Turkey	privacy@tr.webhelp.com
329.	Teknofix Telekomünikasyon ve Bilişim Hizmetleri A.Ş. Ankara Basinevleri Branch (Teknofix Telecomunication and Information Services Joint Stock Company)	Basınevleri Mah. Yankılar Sok. No:16 Keçiören, Ankara	Turkey	privacy@tr.webhelp.com
330.	Telecom Service Centres Ltd	11 Central Park Avenue, Central Business Park, Larbert, Falkirk, FK5 4RX,	United-Kingdom	privacy@uk.webhelp.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
331.	Webhelp Payment Services UK Ltd	C/o Civvals Limited, 50 Seymour Street, London W1H 7JG	United-Kingdom	privacy@wps.webhelp.com
332.	Webhelp Medica UK Limited	Building 2, 1 Nunnery Square, S2 5DD, Sheffield	United-Kingdom	privacy@webhelpmedica.com
333.	Webhelp USA Group Inc	1111 Brickell Avenue, Suite 11, FL 33131, Miami	USA	protecciondedatos@onelinkbpo.com
334.	Webhelp USA LLC	1111 Brickell Avenue, Suite 11, FL 33131, Miami	USA	protecciondedatos@onelinkbpo.com
335.	Webhelp US LLC	1111 Brickell Avenue, Suite 11, FL 33131, Miami	USA	protecciondedatos@onelinkbpo.com
336.	Webhelp Logbox USA	110 West 40th Street , Suite 1903 New York, NY 10018	USA	protecciondedatos@onelinkbpo.com
337.	Webhelp Americas LLC	80 SW 8TH ST, SUITE 2900, FL 33130, Miami	USA	protecciondedatos@onelinkbpo.com
338.	Webhelp California Inc.	200 Madison Avenue, Suite, 1901, NY 10016,New York	USA	protecciondedatos@onelinkbpo.com

DOCUMENT CONTROL

Version	Update	Modifications Summary
0.1	27/02/2022	Final Approval
0.2	02/02/2023	Reviewed list based on dissolution and new entities
0.3	01/04/2024	Re-branding and formatting BCR member updates (reflecting liquidated former BCR Members, new entities and change of names)

Review Frequency	This document will be reviewed at least annually or upon change
Date of Issue	25/05/2018
Domain	Privacy
Classification	Public
Reference	BCR Appendix 1_List of BCR Members and local privacy contacts

17.7
17.8
17.9
17.10

17.11
17.12 Appendix 2
17.13 Definitions for BCR and Procedures

“Applicable Data Protection Legislation”	Means in the following order of prevalence (i) the European Regulation 2016/679 relating to the Processing of Personal Data as of its date of application (“GDPR”), (ii) EU Member States national laws and regulations relating the Processing of Personal Data and implementing GDPR and (iii) any regulation relating to the Processing of Personal Data applicable during the term of this Privacy Policy.
“Binding Corporate Rule” or BCR	Means Personal Data protection policies and procedures which are adhered to by BCR Members for transfers or a set of transfers of Personal Data to a Data Controller or Data Processor in one or more third countries within the Concentrix group.
“BCR Member”	Means any affiliate of the Concentrix group that signed and bound b y the thhe BCR-C and/or BCR-P and as such committed to comply with such BCR, BCR Members are listed in Appendix 01 of such BCR-C and BCR-P.
“Client”	Means any third party, contracting with Concentrix and acting as Data Controller, whose Personal Data is Processed by a BCR Member acting as Data Processor accordingly with its documented instructions.
“Competent SA” or “Competent Supervisory Authority”	Means the EEA Supervisory Authority for the Data Exporter
“Data” or “Information”	Means any kind of information which is individually accessible by electronic or other means such as, but not limited to, logs, Personal Data, documents or other materials.
“Database”	Means a collection of independent works, data, Information or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.
"Data Exporter"	Means the Data Controller or Data Processor Transferring the Personal Data to a non-EEA third country
“Data Importer”	Means the Data Controller or Data Processor receiving the Personal Data
“Data Controller” or “Controller”	Means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determine the purposes and means of the Processing of Personal Data.
“Data Processor” or “Processor”	means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.
“Data Subject”	Means any natural person, who can be identified, directly or indirectly, by means reasonably likely to be used by any natural

	or legal person, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
"Device"	Means any Programmable object that can automatically perform a sequence of calculations or other sequence of operations on Data once programmed directly or indirectly for the task. Any electronic apparatus adapted for displaying in a readable format, Information. Devices include but are not limited to computers, smartphone, tablets, laptops, servers, Networks, telephony platforms etc.
EEA	Means the European Economic Area. Countries that are part of the EEA are the EU Member States as well as Iceland, Liechtenstein and Norway.
"EEA Supervisory Authority"	Means an independent public data protection authority which is established in an EEA Member State.
"Encryption"	Means a process to obfuscate data by transforming Data into a form in which there is a low probability of assigning a meaning or making it readable except when used in conjunction with a confidential process or key to decode it. Such process could be, but are not limited to mathematical function or algorithmic process
"Information Administrator"	Means the natural person within Concentrix organisation, alone or jointly with others, processes or manipulates the Information in accordance with the Information Owner needs', the objectives', purposes' and rules'.
"Information Owner"	Means the natural person within Concentrix organisation which, alone or jointly with others, determines the needs, the objective, purposes and rules of a project including Information processing.
"Intragroup Data Transfer Agreement"	Means the intra-group agreement which comprises the BCR-C and the BCR-P as appendices that all BCR Members are required to execute in order to be bound by the BCR-C and BCR-P
"Information Systems"	Means any Device used directly or indirectly by a User or another Device in order to process Information including, but not limited toc collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of Data

“Local Privacy Leader”	Means the person being the main point of contact of the DPO and dealing with data protection matters within each BCR Member.
“Malicious Software”	Means software that by its introduction, adversely affects the intended function of software/hardware. This could include but is not limited to virus, malware, trojans, ransomware etc.
“Networks”	Means the physical or logical connectivity that allows two or more Devices to communicate.
“Password” or “Passphrase”	Means a string of characters or any other logical or physical means used in conjunction with a User Identity during an authentication process to prove identity of a User and/or grand access to certain Information.
“Personal Data”	Means any information relating to an identified or identifiable natural person, (a Data Subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal Data includes Sensitive Personal Data.
“Personal Data Breach”	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed;
“Privacy Committee”	Means the internal board committee supporting the GlobalData Privacy Officer
“Processing” or “Processed”	Means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
“Pseudonymisation”	Means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data is not attributed to an identified or identifiable natural person;
“Risk”	Means a scenario describing an event and its consequences, estimated in terms of severity and likelihood.
“Risk management”	Means the coordinated activities to direct and control an organization with regard to risk.

“Security Incident”	Means attempted or successful unauthorised access, use, disclosure, modification, or destruction of Information or interference with system operations in the Information System.
“Sensitive Personal Data”	Means special categories of Personal Data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms requiring such Personal Data to merit specific protection as the context of their Processing could create significant risks to the fundamental rights and freedoms – such as Personal Data that reveals racial or ethnic origin, political opinion, religious or philosophical beliefs, or trade union employees, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person’s sexual orientation.
“Service Agreement”	Means the agreement entered into between a Concentrix affiliate and its Client pursuant to which such Concentrix affiliate provides services to its Client.
“Sub-Processor”	Means the entity engaged by a Data Processor for carrying out specific proces sing activities on behalf of the Data Controller, bound by the same data protection obligations as set out in the contract or other legal act between the Data Controller and the Data Processor
“Software” or “Application”	Means any code, instruction, programs routines that allows directly or remotely the manipulation of Data through any means and includes API, command shells etc.
“Transfer of Personal Data”	Means the Processing, material transfer or distant access to Personal Data from entities established outside of the European Economic Area (EEA).
“User”	Means all Concentrix employees, third parties, third parties’ employees, contractors, contractors’ employees and other persons whose conduct and duties allows the access to Concentrix Information Systems.
“Concentrix” or “Concentrix Group”	For the BCR and the related Procedures Concentrix shall mean Webhelp SAS and all entities listed in the List of entities bound by the BCR and are therefore BCR Members

DOCUMENT CONTROL

Version	Update	Modifications Summary
0.1	27/02/2022	Final Approval
0.2	01/04/2024	Re-branding and formatting Alignment with EDPB Recommendations 1/2022 repealing and replacing WP256_Rev01

Review Frequency	This document will be reviewed at least annually or upon change
Date of Issue	25/05/2018
Domain	Privacy
Classification	Public
Reference	BCR Appendix 2 Definitions for BCR and Procedures

Appendix 5
Controller Data Subjects and complaints handling procedure

Table of content

1. Introduction

The adoption of the BCR by the Concentrix group and the commitment from the BCR Members to comply therewith demonstrates BCR Memebrs' commitment to providing a high level of protection to the Personal Data it processes. Concentrix is committed to conducting business in accordance with the Applicable Data Protection Legislation including the European Regulation 2016/679 relating to the processing of Personal Data as of its date of application Concentrix has implemented the following procedure.

The capitalised terms used herein shall have the same meaning as specified under Appendix 2 of the BCR.

2. Objectives of the Procedure

Data Subjects, including employees of BCR Members, are granted specific rights regarding the processing of their Personal Data as further defined under Section 7 of the BCR

When acting as Data Controller, BCR Members shall ensure that any request or complaint from Data Subject in relation to the exercise of their rights ("**Requests**") is addressed in a timely manner as defined hereunder, in order to comply with the BCR and Applicable Data Protection Legislation.

This document describes how BCR Members shall handle a Data Subject's Request where a BCR Member acts as Data Controller (stakeholders, steps and timeline). Where the Request is received from the Data Subjects and that Personal Data is processed by Concentrix BCR Member on behalf of one of Concentrix BCR Members' clients, all requests shall be handled according to the procedure specifically defined under **Appendix 06 - Procedures for handling Data Subjects' requests where Concentrix acts as Data Processor**.

3. Procedures

As a preliminary step, tthe BCRMembers shall expressly inform Data Subjects that they can exercise their rights in accordance with the provisions of Article 7 of he BCR.

3.1 Contact and acknowledgement of receipt of Request

3.1.1 Standard procedure

BCR Members shall also specify how such rights can be exercised. For this purpose, BCR Members will provide Data Subjects with accessible means to exercise their rights and, in particular a single dedicated contact email to be used irrespective of the country a Data Subject is located in. Therefore, any Request as part of this procedure may be sent directly at the following address: dpo@concentrix.com - local emails can be used in order to take into account local specificity, such as language.

On receipt of a Request, the Group Data Privacy Officer ("**DPO**"), or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the following duties, shall ensure they acknowledge receipt thereof no later than 3 working days after the Request was received.

3.1.2 Exception

In the event a complaint from a Data Subject is raised through a different channel than the one described above, the BCR Member or function receiving the complaint shall immediately upon becoming aware, contact the DPO, and (1) internal postal services; (2) Local Privacy Leaders; (3) Business Privacy Referent; and (4) HR departments shall be informed of such procedure.

The Group Data Privacy Officer, or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the following duties shall acknowledge receipt of the matter in writing within 2 working days as from the notification by the function.

3.2 Information collection

Prior to transferring a Request internally, the Group Data Privacy Officer, or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the following duties, shall (1) ensure that they have obtained the minimum required information from the concerned Data Subject to address his/her Request (2), if deemed necessary, obtain as much information as possible to enable that the Request to be duly handled.

As a minimum, and to the extent possible, it shall obtain the following information ("**Minimum Information**"):

- First and last name of the Data Subject; and
- Where legally permitted/requested, copy of the Data Subject's ID or any other document required as a proof of identity; and
- Contact details to be used for reverting to the Data Subject; and
- The Personal Data concerned by the Request and the subject matter of the latter; and
- Date when Personal Data where initially collected; and
- Type of right that the Data Subject wants to exercise (please indicate whether access, deletion, blocking or correction).

If deemed necessary, BCE Members shall obtain the following information:

- BCR Member which initially collected the Personal Data; and
- Category of processing in relation to which the Data Subject is submitting his/her Request;
- Any relevant details regarding the Request.

In order to obtain the necessary information, the BCR Member can invite the Data Subject, who has not specified sufficient information in their email, to further complete a question form, with free text field, or any other means introduced by Concentrix to facilitate the required information collection from the Data Subject. (e.g. pre-fill form field, options available through checkbox etc.). Means allowing collection of data shall, at a minimum, indicate (1) if the answer is mandatory or not and (2) the consequences if answer is not provided.

3.3 Request assessment

The DPO, or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the following duties, shall assess if they have obtained the Minimum Information for handling the Request.

Based on the information requested and obtained, the DPO shall assess the Request. If he/she considers that the Request is reasonable and legitimate (as opposed to a Request with no proof of the Data Subject identity, an excessive demand resulting from repetitive Requests, Request of data already deleted according to the retention period, Requests on behalf of others, career forecast data, etc.) then:

The DPO shall (i) document any Request received and (ii) make the relevant assessment of the Request. In order to properly assess the Request, the DPO, or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the hereinabove duties may need to answer to the following questions:

- What is the nature of the Request? (access, deletion, opposition, rectification, portability) ;
- Do I have enough information to identify the Data Subject? ;
- Do I have enough information regarding the scope of the Request? (geographical and material scope) ;
- Does the Data Subject already have possession or easy access to the requested data (e.g., through Concentrix systems)? ;
- Does the Request include information which is not in a clear format for Data Subjects? If yes, make sure you explain the codes so that the information can be understood;
- Is the Data Subject Request based on a legitimate interest? ;
- Is it technically possible to address the Data Subject's Request (given in particular the volume of data at stake)? ;
- Are third parties involved in the processing of Data Subjects' Personal Data within the scope of the Request? ;
- Would the handling of the Request imply that third parties' Personal Data would need to be communicated to the Data Subject? If yes, is it possible to only extract the Personal Data of the requestor, with reasonable efforts and without a risk for the third parties' Personal Data? If no, this Personal Data cannot be communicated to the Data Subject.

3.4 Answer type identification

On this basis, one can contemplate three different cases:

3.4.1 Case 1

Where the information provided by the Data Subject **is not sufficient** to handle the Request, the DPO, or any other individual or entity, internal or external appointed by the DPO for the purpose of managing the following duties, shall send a request for additional information to the Data Subject no later than 10 working days after receiving the Request.

Where the Request is too complex and subject to compliance with any legal requirement, the timeline of the response may be extended up to 2 months, subject to documentation of the assessment of the complexity by the DPO.

3.4.2 Case 2

Where the DPO considers in their initial assessment, that the Request may **not be legitimate as described in section 3.7**, he/she shall not immediately close the case. The Group Data Protection Officer, or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the following duties shall reply to the Data Subject within 10 working days after receiving the Request, by asking the Data Subject to provide further explanations as to why the Data Subject intends to exercise its rights.

Where necessary, the DPO may inform the relevant stakeholders at local level and the Local Privacy Leader.

Upon receipt of further justification regarding the legitimacy of the Request, the DPO, or the Local Privacy Leader shall, within 15 working days after receiving the information from the Data Subject, (1) make sure that it responds to the Request, or (2) Where he or she considers during the first analysis that the Request addressed by the Data Subject is not legitimate, document why it considers the Request not legitimate and reply to the Data Subject.

Guidance for assessing the legitimacy of the Request is provided above of such procedure. The response shall include the reason for not taking an action and the possibility for the Data Subject to lodge a complaint with a data protection authority and to seek a judicial remedy.

Where the DPO or the relevant privacy network member (i.e., Regional and/or Local Provacy Leader) considers that, based on the additional elements, the Request can be handled it shall ensure that it responds to the Data Subject within the above mentioned 15 working days. Where the Request is too complex and subject to compliance with any legal requirement, the timeline of the response may be extended up to 2 months, subject to documentation of the assessment of the complexity by the DPO.

3.4.3 Case 3

Where information provided by the Data Subject is sufficient, the DPO shall make sure that it responds to the Request without undue delay and maximum **1 month from the receipt of the Request.**

Please note that in any case the response to a data subject must occur within 1 month at the latest after receiving the request (except in certain and limited circumstances as further detailed herein).

3.5 Local mandatory provisions

The Local Privacy Leader, if not directly appointed by the DPO for the purpose of managing the answers to Requests received by a BCR Member, shall be ready to cooperate with the DPO by providing the latter with any relevant information in relation to the matter. The DPO shall then give guidance as to how to handle the case, by taking into account the local circumstances, within 7 working days after receiving the information from the Local Privacy Leader.

3.6 Escalation process

Where the Data Subject is not satisfied with the initial response provided by the Local Privacy Leader or the DPO, and resulting from the handling procedure

described above, such Data Subject shall be entitled in any case to immediately ask for his or her Request to be re-examined.

Data Subject shall provide to the BCR Member a detailed explanation of the unsatisfactory provisions of the solution previously provided. DPO shall inform the Privacy Committeel of such request, and allow the Privacy Committee to proceed to the analysis of such request.

Taking into consideration the analysis provided by the Privacy Committee, and without disclosing such analysis to the Data Subject, the DPO, shall take no longer than 2 months from receipt of the Request for re-examination to determine how it shall be handled and shall inform the Data Subject in writing accordingly.

3.7 Refusal of a Request

Although BCR Members are committed to handling Data Subject Requests efficiently, under certain circumstances, BCR Members may be entitled not to accept a Data Subject's Request.

BCR Members are entitled to decline a Data Subject's Request, where accessing the Data Subject's Request would actually or potentially mean that the following information would be shared with the Data Subject:

- information covered by legal privilege;
- information which a BCR Member is legally forbidden to communicate;
- information BCR Members are processing during the course of an ongoing investigation or pending litigation procedure.

Where information/Personal Data regarding other Data Subjects is visible, data may be redacted before it is shared with the Data Subject.

In addition, where a Data Subject objects further processing of his/her Personal Data and/or asks for the deletion of his/her Personal Data, BCR Members may decline such Request where there is a legal obligation on, or an over-riding legitimate interest for a BCR Member to retain the Personal Data. This shall be assessed on a case by case basis and duly documented.

In any case, if a Data Subject Request or complaint is rejected by a BCR Member or the answer does not satisfy the Data Subject, the Data Subject can contact the DPO and / or can directly lodge a complaint with its competent Supervisory Authority.

3.8 Communication with Data Subjects

When communicating with the Data Subject, BCR Members shall cooperate with the Data Subject and address any Request in a timely manner. All communication shall be provided using clear and plain language, in an intelligible, concise, easily accessible and understandable form.

The information to be provided to Data Subjects shall be accurate and limited to (i) what the Data Subject has requested and (ii) the list of information that may be provided by a Data Controller according to the Applicable Data Protection Legislation.

As a general rule, BCR Members shall not apply fees for reasonable Data Subject Requests. However, under certain circumstances, in particular where the handling of the Request would require significant effort froma BCR Member, reasonable

fees, subject to a national maximum according to applicable laws, may apply provided that the Data Subject is informed about such fees in advance.

-

Questions regarding this procedure or knowledge of a violation or potential violation of this procedure must be reported directly to the Group Data Protection Officer.

DOCUMENT CONTROL

Version	Update	Modifications Summary
0.1	27/02/2022	Final Approval
0.2	19/05/2023	New postal address of Webhelp SAS / Group DPO
0.3	01/04/2024	Re-branding and formatting

Review Frequency	This document will be reviewed at least annually or upon change
Date of Issue	25/05/2018
Domain	Privacy
Classification	Confidential
Reference	BCR Appendix 5_Controller Data Subjects' request and complaints handling procedure

Appendix 6
Processor Data Subjects' request and complaints handling procedure

Table of content

1.Introduction

The adoption of the Binding Corporate Rules ("BCR")and the commitment from the BCR Members to comply therewith demonstrates BCR Members' commitment to providing a high level of protection to the Personal Data it processes. BCR Members are committed to conducting business in accordance with the Applicable Data Protection Legislation including the European Regulation 2016/679 relating to the processing of Personal Data as of its date of application, any regulation relating to the processing of Personal Data applicable during the term of the Privacy Policy. As a consequence, Concentrix has implemented the following procedure.

The capitalised terms used herein shall have the same meaning as specified under Appendix 2 – Privacy definitions for BCR and Procedure of the the BCR.

2. Objectives of the Procedure

Data Subjects, including employees of BCR Members, are granted specific rights regarding the processing of their Personal Data as further defined under Article 7 of the BCR.

When acting as Data Processor, BCR Members shall ensure that any request or complaint from Data Subject in relation to the exercise of their rights ("**Requests**") is addressed in a timely manner as defined hereunder, in order to comply with the BCR and Applicable Data Protection Legislation. However, this shall only apply where BCR Members actually processes the requested information.

This document describes how BCR Members shall handle a Data Subject's Request where acting as Data Processor (stakeholders, steps and timeline). Conversely, the Requests received from Data Subjects whose Personal Data is processed by a BCR Member on its own behalf only, as a Data Controller, shall be handled according to the procedure specifically defined under the Policies and **Procedure 05 - Controller Data Subjects' requests and complaints handling procedure**In most cases, a Request from an individual (e.g. a Client's employee, client end user) will fall within the following situation:

- The Processing conditions are not compliant with the Applicable Data Protection Legislation (e.g., health data not used, stored and/or encrypted in accordance with the local healthcare applicable law);
- The individual would like to exercise his/her privacy rights according to the Applicable Data Protection Legislation such as:
  - Accessing the Personal Data relating to him/her and processed by BCR Members on behalf of the Client they entered into a relation with;
  - Obtaining rectification, deletion or suspension of any inaccurate or incomplete Personal Data relating to him/her, or which is no longer processed for a valid or appropriate purpose;
  - Objecting to the processing of his/her Personal Data at any time, unless such processing is required by applicable law, provided that the individual demonstrates that he/she has a legitimate ground to object as it pertains to his/her particular situation; and
  - Receiving his/her Personal Data in a structured, commonly used and machine-readable format.

Even if such individual does not have a direct into relationship with Concentrix, there may be cases where BCR Members receive a Request directly from the individual and/or is asked by the Client to handle the Request on its behalf. **BCR Members shall in any case refer to the engagement with the Client to check whether specific conditions apply as to the handling of the Request** (e.g., interdiction to communicate directly with the Data Subjects etc.).

As a consequence, the cost and technical impacts of the Request must be anticipated and addressed at the beginning of each engagement.

3. Procedures

Concentrix, acting as a Processor, is not responsible for informing Data Subjects of their rights in relation to Personal Data. Unless otherwise determined by applicable laws and regulation, such obligations are the responsibility of the Data Controller. Notwithstanding the above, BCR Members are committed to provide sufficient guarantees by implementing appropriate technical and organisational measures in such a manner that Processing of Personal Data on behalf of the Data Controller will meet applicable requirements and ensure the protection of the rights of the Data Subject. Therefore, the procedures below apply where Concentrix acts as Data Processor on behalf of a Data Controller.

Since, it cannot formally be excluded that a Data Subject would send his/her Request directly to a BCR Member, two different cases have to be considered.

3.1. Request directly received by a BCR Member

3.1.1. Internal communication

Any Request in relation to Personal Data that Concentrix processes as Data Processor (e.g., on behalf of its Clients) received by an employee or workforce of a BCR Member must **immediately be** communicated to the Local Privacy Leader or Business Privacy Referent. Business Privacy Referent shall immediately inform the Local Privacy Leader,.

As a matter of efficiency, such Request can also be communicated to the DPO through the following email:

dpo@concentrix.com

The latter will then allocate the Request to the relevant Local Privacy Leader no later than 1 working day after receipt thereof.

The information provided by the employee or workforce of Concentrix must at least specify the following information:

- Name of the local manager in charge of the Client account;
- Copy of the Request; and
- Name of the Client the Data Subject's relates to.

Business Privacy Referent shall immediately inform its Local Privacy Leader

3.1.2. Transfer of the Request to the Client

Once it receives such Request, the Local Privacy Leader, will draft a communication to the Client about the Request. Such communication must (1) be sent by the Local Privacy Leader to the Client, in cooperation with the local manager in charge of the relationship with the Client; and (2) no later than 2 working days after receiving the Request. The Local Privacy Leader will also inform the DPO that the Request has been transferred to the Client.

3.1.3. BCR Member's assistance to the Client.

At the same time, the Local Privacy Leader, with the support of the operations and account management teams, shall assess and verify if Concentrix actually processes the Personal Data of the Data Subject addressing the Request.

No answer shall be provided without Client's instructions

Should the Client allow BCR Members to handle the Request on its behalf, the Local the BCR Member Leader shall determine with the Client whether the Client itself or the BCR Member shall acknowledge receipt of the Request and inform the Data Subject of BCR Member role in the processing of his/her Request.

Unless otherwise expressly instructed by the Client, BCR Members shall not enter into contact with the Data Subject during the entire procedure.

3.2. Request sent by the Data Controller to a BCR Member

3.2.1. Internal communication

Any Request in relation to Personal Data that Concentrix processes as Data Processor (e.g., on behalf of its Clients) received by an employee or workforce of from a Client must **immediately be** communicated to the Local Privacy Leader or Business Privacy Referent. Business Privacy Referent shall immediately inform its Local Privacy Leader.

Where a Client sends to a BCR Member a Data Subject's Request regarding the processing of his/her Personal Data to handle, the BCR Member shall acknowledge receipt thereof to the Client no later than 2 working days after receiving such Request.

No later than 5 working days after the reception of the Request, the BCR Member must verify the extent to which it can address and handle the Request.

3.2.2. Request Assessment

Upon receipt of a Request, either directly from the Data Subject or from the Client, and subject to the provisions and steps described in this Procedure, the Local Privacy Leader, or any other individual or entity, internal or external, appointed by the Local Privacy Leader for the purpose of managing the following duties shall ensure and verify that he/she has all information necessary from the Client and the Data Subject to address his/her Request, in particular:

- Does the provided information allow the BCR Member to identify the Data Subject? (i.e. Name and first name of the Data Subject);
- Description of the context in which the Personal Data was collected (if possible)
- Is the BCR Member authorised to handle the Request on behalf of the Client?
- What is the nature of the Request? (access, deletion, opposition, rectification, portability)
- Does the Client consider the Data Subject's Request reasonable?
- Is it technically possible to address the Data Subject's Request (given in particular the volume of data at stake)?
- Does the BCR Member have enough information regarding the scope of the Request? (geographical and material scope, Approximate date the Data was collected;)
- Does the Data Subject already have possession or easy access to the requested Personal Data?
- Does the Request include information which is not in a clear format for Data Subjects? If yes, make sure you explain the codes so that the information can be understood.

- Are third parties involved in the processing of Data Subjects' Personal Data within the scope of the Request?
- Would the handling of the Request imply that third parties' Personal Data would need to be communicated to the Data Subject? If yes, is it possible to only extract the Personal Data of the requestor, with reasonable efforts and without a risk for the third parties' Personal Data?

Noteworthy, the gathering of such information must be limited to what is currently available within Concentrix. No additional information will be collected.

BCR Members **shall refrain as much as possible from communicating with the Data Subject even if required by the Client. Where such request is sent to a BCR Member, the latter shall first discuss with the Client the real opportunity to have Concentrix entering directly into contact with the Data Subject. If the BCR Member accepts direct contacts with the Data Subject, such BCR Member must inform the Client that the latter retains the entire responsibility vis-à-vis the Data Subject for handling in due course such Request.**

3.2.3. Answer type identification

The Local Privacy Leader shall make sure that it examines the information provided by the Client and by the Data Subject within 8 working days from the time it receives the Request to determine if:

- He/she has the appropriate information to handle the Request; and
- He/she considers that the Request is reasonable (as opposed to a Request with no proof of the Data Subject identity, an excessive demand resulting from repetitive Requests, Request of Personal Data already deleted according to the retention period, Requests on behalf of others, etc.).

Three cases are then possible. These are as follows:

(viii) **Case 1**

Where the information provided by the Data Subject **is not sufficient** to handle the Request, the Local Privacy Leader, or any other individual or entity, internal or external appointed by the Local Privacy Leader for the purpose of managing the following duties, shall send a request for additional information to the Client no later than 2 working days after receiving the Request.

Where the Request is too complex, and subject to compliance with any legal requirement, the timeline of the response may be extended up to **20 working days**, subject to documentation of the assessment of the complexity by the Local Privacy Leader.

(ix) **Case 2**

Where the Local Privacy Leader considers on initial assessment, that the Request may **not be reasonable**, he/she shall not immediately close the case. The Local Privacy Leader, or any other individual or entity, internal or external, appointed by the Local Privacy Leader for the purpose of managing the following duties, shall reply to the Client **within 10 working days** after receiving the Request, by asking the Client to provide additional information as to why the Data Subject intends to exercise its rights.

Upon receipt of additional information, where the Local Privacy Leader still considers that the Request addressed by the Data Subject is not reasonable, the Local Privacy Leader shall document why it considers the Request is not reasonable

and shall ensure, after approval of the DPO in writing, to reply to the Client or Data Subject, if expressly instructed by the Client, no later than **15 working days** after receiving the additional information.

The response shall include the reason for not taking an action and the possibility for the Data Subject to lodge a complaint with a data protection authority and seek a judicial remedy. The wording of such response shall be validated by the DPO and the Client.

Where the Local Privacy Leader considers that, based on the additional elements, the Request can be handled it shall ensure that it addresses the request within the above mentioned **15 working days** and shall inform the DPO accordingly.

(x) **Case 3**

Where information provided by the Client and/or the Data Subject is sufficient, the Local Privacy Leader shall make sure that it responds to the Request, pursuant to the instructions of the Client, within **15 working days** from the receipt thereof and duly informs in writing the DPO about the timing and content of the response so provided.

3.2.4. Escalation process

In the case of a complaint received directly from a Data Subject as to how its Request has been addressed, whether during or after the response has been given, the Local Privacy Leader shall ensure that it shares with the Client and the DPO the matter, **no later than 3 working** days after receiving the Data Subject's complaint.

For each of the above steps, and where necessary to handle the case appropriately, the Local Privacy Leader shall be ready to cooperate with the DPO by providing the latter with any relevant information in relation to the matter and inform the Client of the handling of the procedure.

The Group Data Protection Officer's guidance shall be binding. However, the DPO shall not enter into contact directly with the Data Subject, unless expressly required by the Client and the Local Privacy Leader.

3.2.5. Refusal of a Request

Although BCR Members are committed to handling Data Subjects' Requests efficiently, under certain circumstances as defined below, BCR Members may be entitled not to accept the Client or Data Subject Request.

BCR Members can oppose the Client's or Data Subject's Request, where agreeing to the Request would imply that the following information would be shared:

- information covered by the legal privilege;
- information which a BCR Member is legally forbidden to communicate; and/or
- information a BCR Member is processing during the course of an ongoing investigation or pending litigation procedure.

Where there is a conflict of privacy, Personal Data may be redacted before it is shared with the Client or the Data Subject.

In addition, in case of a Request received from the Client regarding a Data Subject opposing the further processing of his/her Personal Data and/or asking for the deletion of his/her Personal Data, BCR Members may refuse to grant such Request where legal obligations prevent BCR Members from doing so or where BCR

Members have an over-riding legitimate interest. This shall be assessed on a case by case basis and referred to the DPO for a final decision before the Client or the Data Subject is informed.

3.2.6. Communication with Data Subjects

If the Client requires BCR Members to handle the Request on its behalf, the following rules shall apply when BCR Members communicate with the Data Subject.

Under no circumstances and unless otherwise expressly instructed by the Client, shall BCR Members enter into contact with the Data Subject during the entire procedure. Even if required by the Client, BCR Members shall refrain as much as possible from communicating with the Data Subject.

When communicating with the Data Subject, BCR Members shall cooperate with the Data Subject and address any Request in a timely manner. All communication shall be provided using clear and plain language, in an intelligible, concise, easily accessible and understandable form.

The information to be provided to Data Subjects shall be accurate and limited to (i) what the Data Subject has requested and (ii) the list of information that may be provided by a Data Controller according to the Applicable Data Protection Legislation.

The Local Privacy Leader shall pay particular attention to the deadlines mentioned in this Procedure.

As a general rule, BCR Members shall not apply fees for reasonable Data Subject Requests. However, under certain circumstances, in particular where the handling of the Request would imply important efforts from BCR Members , reasonable fees, subject to a national maximum according to applicable laws, may apply provided that the Data Subject is informed about such fees in advance.

-

Questions regarding this procedure or knowledge of a violation or potential violation of this procedure must be reported directly to the Group Data Protection Officer.

-

DOCUMENT CONTROL

Version	Update	Modifications Summary
0.1	27/02/2022	Final Approval
0.2	19/05/2023	New postal address of Webhelp SAS / Group DPO
0.3	01/04/2024	Re-branding and formatting

Review Frequency	This document will be reviewed at least annually or upon change
Date of Issue	25/05/2018
Domain	Privacy
Classification	Confidential
Reference	BCR Appendix 6_ Processor Data Subjects' requests and complaints handling procedure

Appendix 11A
Material Scope of the BCR Controller
List of Purposes of Processing and related Categories of Personal Data and Data Subjects

In addition to the provisions of section 2.1 on the material scope of this BCR-C, the table below provides further details on the Transfers performed under this BCR-C. This table details on the Purpose of Processing and the related categories of Data Subjects and Personal data covered by the present BCR-C. The table provided in section 1 below gives details about the transfers of personal data carried out between BCR Members listed in Appendix 1 under this BCR-C.

The countries to which the Personal Data may be transferred depend on the localization of BCR Members involved in the Processing activities and is provided in Appendix 1. Note that as regard BCR-C, Transfers of Personal Data mostly occur between the BCR Members of a same Region (except for the Global entities where there may be transfers between such Global entities and all other BCR Members depending on the Purposes of Processing. For more transparency, we have included an additional table presenting the Regions in section 2 of the present Appendix.

1. Table on Transfers of Personal Data between BCR Members listed in Appendix 1 under this BCR-C

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
HR processing activities	**Recruitment management**	**1.Identification data** (e.g., Name, Last name. E-Mail, Phone number, picture (if provided), Address) **2. Economic and financial data** (e.g., salary expectation) **3. Professional data** (e.g., CV-resume Previous experience, Diplomas, certificates, foreign languages spoken, assessment of knowledge and trainings, number and copy of their work permit (only if necessary)) **4. Background check** (results of background check (only the results,	**Candidates**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
		and for successful candidates to be hired)	
	Employee records management (incl. Onboarding process, maintenance of employee record in accordance with the applicable legislation, administrative follow-up of occupational medicine, internal directory)	**1.Identification data** (e.g., Name, Last name, E-Mail, Phone number, picture of the data subject, Address, Gender, family status) **2.Professional data** (e.g., CV-Resume , Educational records and information regarding skills of the employee, Previous experience, Diplomas/certificates, foreign languages spoken, assessment of knowledge and trainings, number and copy of their work permit (only if necessary), Employee internal identification number, office location, previous work history, Business Unit Division Line Reporting Manager, contract type) **3.Economic and financial data** (e.g., Income/Salary, IBAN/BIC) **4. Sensitive data** (social security number)	**BCR Members' employees**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
	Payroll Management	**1.Identification data** (e.g., Name, Last name, E-Mail, Phone number, Address) **2. Professional data** (e.g., Employee internal identification number, contract type, hours of work) **3. Economic and financial data** (e.g., Payment data (worked hours, absences, compensation and benefits, bonus, Benefits and Entitlements Data), salary wage, IBAN/BIC) **4.Sensitive data** (Social Security number)	**BCR Members' employees**
	Referral Program management	**1. Identification data** (e.g., Name, Last name, E-Mail, Phone number, Address). **2. Professional data** (e.g., CV-resume Previous experience, Diplomas, certificates, foreign languages spoken, assessment of knowledge and trainings).	**BCR Members' employees Candidates**
	Badge management for employees	**1.Identification data** (e.g., Name, last name, phone number) **2.Professional data** (e.g., job title role, Employee internal identification number), Employee badge number, authorized areas and working hours)	**BCR Members' employees**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
		3.Economic and financial data (e.g., payment attached to the use of the canteen)	
	Employee's training management (incl. Internal training and client's training)	**1.Identification data** (e.g., Name, Last name, E-Mail, Phone number, Address) **2.Professional data** (e.g., Job title role, Employee internal identification number, Training information (type of training, date, attendance, quiz results, etc.), office location, previous work history Business Unit Division, line Reporting Manager)	**BCR Members' employees**
	Employee's career and mobility management	**1.Identification data** (e.g., Name, Last name . E-Mail, Phone number, picture (if provided), Address) **2. Professional data** (e.g., CV-resume, Current job title role, Previous experience, Diplomas, certificates, foreign languages spoken, assessment of knowledge and trainings, number and copy of their work permit (only if necessary))	**BCR Members' employees**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
	Employees' background check	**1.Identification data** (e.g., Name, Last name. E-Mail, Phone number, photo (if provided), Address) **2. Professional data** (e.g., CV-resume, Current job title role, Previous experience, Diplomas, certificates, foreign languages spoken, assessment of knowledge and trainings, number and copy of their work permit (only if necessary)) **4. Background check information** (e.g., background check results)	**BCR Members' employees**
	Employees' absence and working time management	**1. Identification data** (e.g., Name, Last name) **2. Professional data** (e.g., Employee internal identification number, office location, previous work history, Business Unit Division Line Reporting Manager, contract type, hours of work, work schedule, absences (sick leaves, vacations, etc.))	**BCR Members' employees**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
	Professional elections management	**1.Identification data** (e.g., Name, Last name, age) **2. Professional data** (e.g., Preparation of the electoral list (identity of voters, age, seniority, college), applications management (identity, nature of the mandate applied for, information allowing to verify compliance with eligibility requirements, if applicable trade-union membership declared by the candidates) and release of the results of the elections (identity of the candidates, mandates concerned, number and percentage of votes obtained, identity of the elected employees and, if applicable, trade-union membership of the elected employees).	**BCR Members' employees**
	Management of Employees representative bodies' committees	**1. Identification data** (e.g., Name, Last name) **2. Professional data** (e.g., Convocations, preparatory documents, reports, various minutes of representative bodies' committee).	**BCR Members' employees**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
	Employees' performance and evaluation management	**1. Identification data** (e.g., Name, Last name). **2. Professional data** (e.g., information on evaluation: dates of the evaluation interviews, identity of the evaluator, professional competencies of the employee, objectives assigned, results objectives, results obtained, assessment of professional skills on the basis of objective criteria with a direct and necessary link to the job, observations and wishes formulated by the employee, career development forecasts. For agents, transcription of call conversation with end customer may be used for quality assessment purposes).	**BCR Members' employees**
	Quality assessment of agents / operators	**1. Identification data** (e.g., Name, Last name, email) **2. Professional data** (e.g., Employee internal identification number, job title role, Line reporting managers, KPIs, objectives assigned, results objectives, results obtained, assessment of professional skills on the basis of objective criteria with a direct and necessary link to the job, observations and wishes formulated by the	**BCR Members' agents/operators**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
		employee, career development forecasts. transcription of call conversation with end customer may be used for quality assessment purposes, evaluation results)	
	Employee Wellbeing Program	**1. Identification data** (e.g., Name, Last name, email) **2. Professional data** (e.g., internal ID number, survey score, care conversation scheduled, job position, line manager, shifts, working hours, quality assessment results, etc.)	**BCR Members' employees (moderators)**
	Impact sourcing program management (recruitment, reporting, etc.)	**1.Identification data** (e.g., Name, Last name . E-Mail, Phone number, photo (if provided), Address) **2. Economic and financial data** (e.g., salary expectation) **3. Professional data** (e.g., CV-resume Previous experience, Diplomas, certificates, foreign languages spoken, assessment of knowledge and trainings, number and copy of their work permit (only if necessary), source of recruitment)	**Candidates, BCR Members' employees**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
	Travel and expenses management	**1. Identification data** (e.g., Name, Last name, Address) **2. Professional data** (e.g., Job title role, employee internal identification number, booking reservation, dates of travel, business justification, line reporting manager) **3. Economic and financial data** (e.g., expenses report, invoices, IBAN / BIC)	**BCR Members' employees**
	Social & cultural activities management	**1. Identification data** (e.g., Name, Last name, Address, marital status/relationship) **2. Professional data** (e.g., Job title role, employee internal identification number) **3. Economic and financial data** (e.g., income, benefits and benefits claimed and provided)	**BCR Members' employees (and their declared relatives)**
Company life & services	**IT Management (IT equipment allocation and management, service desk)**	**1. Identification data** (e.g., Name, Last name email address) **2. Professional data** (e.g., employee internal identification number, job title role, office location, line reporting manager, IT request information (Ticket number, request topic, request follow-up) **3 Technical and connection data** (e.g., IP Address, user account	**BCR Members' employees**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
		information, Device ID, , necessary professional applications and websites)	
	Internal Information Security (Fraud Prevention)	**1. Identification data** (e.g., Name, Last name email address) **2. Professional data** (e.g., employee internal identification number, job title role, office location, line reporting manager) **3 Technical and connection data** (e.g., IP Address, user account information, Device ID, alter, results of alerts)	**BCR Members' Employees**
	CCTV within Concentrix facilities	**1.Identification data** (e.g. footages)	**BCR Members' employees** **Visitors to BCR Members' premises**
	Management of telephony in the workplace	**1. Identification data:** (e.g. name, last name, email address, phone number) **2.Technical and connection data** (e.g., IP Address, Logins, Device ID data, type of phone, relevant information regarding the use of telephony services and data necessary for invoicing purposes, including	**BCR Members' employees**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
		operator, the nature of the call (local, national, international), the duration of the call, the time and date of the beginning and end of the phone call and the invoice)	
	Internal communication to Employees (incl., internal communication by email, or via Virtual private networks (intranet))	**1.Identification data** (e.g., Name, Last name email address). **2.Professional data** (e.g., charts, discussion areas, information areas applications and networks) **.4.Technical and connection data** (e.g., IP Address, Device ID data, user account information)	**BCR Members' employees**
	Employees Survey and form	**1.Identification data** (e.g., Name, Last name email address, phone number) **2.Technical and connection data** (e.g., employee internal identification number, job title role, office location, anonymous & aggregated results)	**BCR Members' employees**
	Internal Directory & Employees' user access and accounts management	**1.Identification data** (e.g., Name, Last name email address). **2.Professional data** (e.g., charts, discussion areas, information areas applications and networks).	**BCR Members' employees**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
		3. Technical and connection data (e.g., IP Address, Device ID data, user account information)	
	Internet access and control and prevention of data loss	**1.Identification data** (e.g., Name, Last name email address) **2.Professional data** (e.g., employee internal identification number, job title role, office location, line reporting manager, authorized application & website, employee job title role) **.4.Technical and connection data** (e.g., IP Address, Device ID data, user account information)	**BCR Members' employees**
Legal / Compliance	**Fraud Prevention and detection**	**1. Identification data** (e.g., Name, Last name, email, phone number). **2. Technical and connection data** (e.g.,IP Address, Logins ,Device ID data, interaction data, bug reports, monitoring information embedded in the application, device used). **3. Interaction data necessary to investigate a potential fraud** (e.g., Identification through the means used to provide the services and contact the End Customers; Voice data of the End Client	**BCR Members' employees** **BCR Members customers/clients**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
		and the Service Provider's employee, transcription of the interaction. Telephone number, email address, operations planning, operations performance indicators and peer performance indicators)	
	Whistleblowing system	**1.Identification data** (e.g., name last name, email, phone number, details of the people author of the alert, of the people subject of the alert and of people involved in the processing of the alert) **2. Professional data** (e.g., contract type, job title role, Function/job of the person(s) reporting the incident, the person(s) implicated in the incident and the person(s) involved in the investigation**)** **3. Information of the alert** (e.g., facts reported, evidence as part of the investigation, record of investigations follow-up of the alert).	**BCR Members' employees and administrators**
	Corporate & Legal entities management *(incl. Mandates and proxy, Delegation of powers and signatures, Corporate reporting (boards,*	**1.Identification data** (e.g., Name or company name, E-Mail , Phone number) **2.Professional data** (e.g., (e.g., CV-Resume , Educational records and information regarding skills of the employee,	**BCR Members' employees and administrators**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
	committees), Professional associations, external counsels directory)	Previous experience, Diplomas/certificates, foreign languages spoken, assessment of knowledge and trainings, number and copy of their work permit (only if necessary), Employee internal identification number, office location, delegation of authorities, proxy) **3.Economic and financial data** (e.g., Payment ,Income/Salary, Financial situation ,invoices, Credit card n umber ,IBAN / BIC)	
	Employees' litigation and disciplinary procedures	**1.Identification data** (e.g., Name, Last name, E-Mail, Phone number, footage (if necessary), Address) **2. Professional data** (e.g., employee internal identification number, office location, line reporting manager, information related to potential disciplinary actions and procedure for employees, nature of litigation for business related litigation, job title role / function) **Information related to the litigation matter** (e.g., subject matter, estimated risks, evidence, etc.)	**BCR Members' employees** **Attorneys**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
	Litigation management	**1.Identification data** (e.g., Name, Last name, E-Mail , Phone number, footage (if necessary), Address) **2. Professional data** (e.g., nature of litigation for business related litigation, job title role / function) Information related to the litigation matter (e.g., subject matter, estimated risks, evidence, etc.)	**BCR Members' employees** **BCR Members' business partners** **Attorneys**
	Clients and business partners database (BtoB)	**1.Identification data** (e.g., Name or company name, E-Mail, Phone number, Address Of headquarters) **2. Professional data** (e.g., job title role) **3.Economic and financial data** (e.g., Payment ,Income/Salary, Financial situation, invoices, Credit card number ,IBAN / BIC)	**BCR Members' Business partners/ Clients**
Operation & Marketing	**Client and prospect leads management**	**1.Identification data** (Name, Last name, E-Mail, Phone number, professional Address) **2.Professional data** (job title, role, company name, office location) **3. Economic and financial data** (client agreement, invoice, dunning, purchase orders).	**BCR Members' Clients/Prospects (business contact)**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
	Concentrix Direct marketing campaigns	**1.Identification data** (Name, Last name, E-Mai, Phone number, professional Address) **2.Professional data** (job title, role, company name, office location, optout decision)	**BCR Members' Clients/Prospects (business contact)**
	Processing of Payment Services - WPS	**1.Identification data** (e.g. Name, Last name ,ID card, E-Mail , Phone number, Postal Address , Gender, internal references) **2.Professional data** (e.g., Information related to the profession, information related to the regulatory qualification of a politically exposed person) **3. Economic and financial data** (e.g. Payment, Income/Salary, Financial situation, invoices, IBAN / BIC)	**BCR Members' Clients/Prospects**
Partner/Vendor relationships	**Suppliers Management and Contract Management**	**1.Identification data** (e.g.,Name , E-Mail , Phone number, Address Of headquarters) **2.Professional data** (e.g., Job titles, copy of supplier agreements, invoice, dunning, purchase orders)	**BCR Members' employess** **Supplier's Business contact**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
	Data broker relationship management	**1.Identification data** (e.g., Name, E-Mail, Phone number, address) **2. Professional data** (e.g., Job title role, line reporting manager, optin/optout, hobbies, contractual relationship, invoice, dunning)	**BCR Members' employees** **Data broker's Business contact Webhelp Client/Prospect (business contact)**

2. Table on BCR Members' Regions

Concentrix Geo/Regions	Countries included in the Geo/ Region
Group (Global)	**All countries*** **Transfers may occur between Global entities (including Global Shared Services entities) and all other BCR Members entities of the Group, whatever their country of location identified in Appendix 1*

AMERICAS	**Canada** **Colombia** **El Salvador** **Guatemala** **Honduras** **Mexico** **Nicaragua** **Peru** **US**
APAC	**Australia** **China** **Hong Kong** **Japan** **Malaysia** **Philippines** **Singapore** **Thailand**
CRIT	**Albania** **Czech Republic** **Italy** **Slovakia**
DACH	**Austria** **Bosnia-Herzegovina** **Bulgaria** **Germany** **Hungary** **Kosovo** **North Macedonia** **Poland** **Slovenia** **Switzerland**

FRANCE	**Algeria** **Benin** **France** **Greece** **Ivory Coast** **Madagascar** **Morocco** **Portugal** **Romania** **Senegal**
MET	**Egypt** **Israel** **Jordan** **Saudi Arabia** **Turkey**
NETHERLANDS	**The Netherlands** **Surinam**
NORDICS	**Denmark** **Estonia** **Finland** **Latvia** **Lithuania** **Norway** **Sweden**
SPAIN	**Spain**
UK	**India** **Sout Africa** **United Kingdom**

WPS/WKS	**Belgium** **France** **Germany** **Italy** **Portugal** **Spain** **United Kingdom** **United States** *Transfers may occur between WPS/WKS affiliates only.*
NETINO	**France** **Madagascar**
WEBHELP MEDICA	**France** **Portugal** **Spain** *Transfers may occur between Webhelp Medica affiliates only.*

DOCUMENT CONTROL

Version	Update	Modifications Summary
0.1	27/02/2022	Final Approval
0.2	19/05/2023	Document control (added) Update of countries and Regions New processing added (wellbeing program)
0.3	01/04/2024	Re-branding and formatting

Review Frequency	This document will be reviewed at least annually or upon change
Date of Issue	25/05/2018
Domain	Privacy
Classification	Public
Reference	BCR Appendix 11A

Appendix 11B
Material Scope of the BCR Processor
List of Purposes of Processing and related Categories of Personal Data and Data Subjects

In addition to the provisions of section 2.1 on the material scope of this BCR-P, the table below provides further details on the transfers performed under this BCR-P. This table details on the Purpose of Processing and the related categories of Data Subjects and Personal data covered by the present BCR-P The table below provides details about the Transfers of Personal Data carried out between BCR Members Entities listed in Appendix 1 under this BCR-P.

The countries to which the personal data may be transferred depend of the localization of BCR Members involved in the processing activities and is provided in Appendix 1.

Domain of processing activities		Purpose of processing	Categories of Personal Data	Categories of Data Subjects
Operation	*Contact centers related activities*	**Contact Center Operations Management**	**1.Identification data** (e.g., Name, Last name, E-Mail ,Phone number, Address, Internal processing code allowing the identification of the End Customer) **2.Professional data** (e.g. ,job title role, employee internal identification number, line reporting manager) **3. Technical and connection data** (e.g., IP Address, Logins, Device ID data) **4. Personal life data (of End-customer)** (e.g., Marital status, number of persons in the household, number and age of children in the household, occupation, living habits and lifestyle, field of activity) **5. Contract management data** (e.g., Transaction number, details of the purchase, subscription, description, and conditions of the good or service purchased, History of the interaction between the End Customer and the Data Controller) **6. Loyalty programs and Outbound activities data** (e.g., Data necessary for the management and cycle of loyalty programs, prospecting, research, surveys, product testing and promotion) **7. Economic and Financial data** (e.g., information necessary to manage end-customer request such as Information on payment, payment terms (discounts, rebates, etc.), bank details)	**BCR Members' employees** **Controller/Client 's End customer / Prospects** **Controller's/ Client's employees and related staff member**

Domain of processing activities		Purpose of processing	Categories of Personal Data	Categories of Data Subjects
		Opt-out operations (in the course of outbound activities)	**1.Identification data** (e.g., Name, Last name, E-Mail ,Phone number, Address, Internal processing code allowing the identification of the End Customer) **2.Technical and connection data** (e.g., IP Address ,Logins ,Device ID data) **3. Contract Management Data** (e.g., Information regarding the Customer's decision to unsubscribe, including via a third party "do not call list)	**BCR Members'employees** **Controller/Client's End customer / Prospects**
		End-Customer satisfaction control	**1.Identification data** (e.g. Identification by the means used to interact with the Contact Center (telephone number, fax number, e-mail address, internal processing code allowing identification of the End-Customer) **2.Professional data** (e.g., job title role, line reporting manager, office location) **3. Technical and connection data** (e.g., IP Address, Logins ,Device ID data) **4. Contract management data** (e.g., aggregated responses provided, results of evaluation)	**BCR Members'employees** **Controller/Client's End customer / Prospects**
		Fraud Prevention and detection	**1. Identification data** (e.g., Name, Last name, E-Mail ,Phone number, Address, Internal processing code allowing the identification of the End Customer) **2. Professional data** (e.g., job title role, line reporting manager, office location) **3. Technical and connection data** (e.g., IP Address, Logins, Device ID data) **4. Interaction data** (e.g., information on end-customer	**BCR Members' employees** **Controller/Client's End customer / Prospects** **Controller's/ Client's employees and related**

Domain of processing activities		Purpose of processing	Categories of Personal Data	Categories of Data Subjects
			request, response provided, transcription of conversation)	**staff member**
		Monitoring, listening & recording interactions	**1. Identification data** (e.g., Name, Last name, E-Mail ,Phone number, Address, Internal processing code allowing the identification of the End Customer) **2. Professional data** (e.g., job title role, line reporting manager, office location, employee internal identification number) **3. Technical and connection data** (e.g., IP Address, Logins, Device ID data) **4. Personal life data** (of End-customer) (e.g., Marital status, number of persons in the household, number and age of children in the household, occupation, living habits and lifestyle, field of activity) **5. Contract management data** (e.g., Transaction number, details of the purchase, subscription, description and conditions of the good or service purchased, History of the interaction between the End Customer and the Data Controller) **6. Loyalty programs and Outbound activities data** (e.g., Data necessary for the management and cycle of loyalty programs, prospecting, research, surveys, product testing and promotion) **7. Economic and Financial data** (e.g., information necessary to manage end-customer request	**BCR Members'employees** **Controller/Client's End customer / Prospects** **Controller's/ Client's employees and related staff member**

Domain of processing activities		Purpose of processing	Categories of Personal Data	Categories of Data Subjects
			such as Information on payment, payment terms (discounts, rebates, etc.), bank details) 8. **Interaction data** (e.g., information on end-customer request, response provided, transcription of conversation)	
		Business Intelligence, reporting and analysis	**1.Identification data** (e.g., name, last name **2.Professional data** (e.g., job title role, line reporting manager, office location) **3. Technical and connection data** (e.g., IP Address, Logins ,Device ID data) **4. Contract management data** (e.g., aggregated stats on compliance with KPI imposed by the client)	**BCR Members' employees** **Controller/Client's End customer / Prospects** **Controller's/ Client's employees and related staff member**
		Numbering & Routing interactions/ interactions technical management	**1. Identification data** (e.g., Name, Last name, E-Mail, Phone number, Address, Internal processing code allowing the identification of the End Customer) **2. Professional data** (e.g., job title role, line reporting manager, office location, employee internal identification number) **3. Technical and connection data** (e.g., IP Address, Logins, Device ID data) **4. Contract management data** (e.g., Information regarding the	**BCR Members"s employees** **Controller/Client's End customer / Prospects**

Domain of processing activities		Purpose of processing	Categories of Personal Data	Categories of Data Subjects
			Customer's decision to unsubscribe, including via a third party "do not call list)	
		Modification of the agent's voice to shape its expressivity and improve communication	**1. Identification data** (e.g., Name, Last name, E-Mail, Phone number, Address) **2. Professional data** (e.g., job title role, line reporting manager, office location, employee internal identification number) **3. Technical and connection data** (e.g., IP Address, Logins, Device ID data)	**BCR Members' employees**
	Netino activities	**Moderation and online social interactions**	**1.Identification data** (e.g, Name, Last name , picture of the end customer (if published on the tool), E-Mail , Phone number, pseudo) **2.Technical and connection data** (e.g., IP Address ,Logins, Device ID data) **3. Interaction data** (e.g., access to data published by the data subject on a platform)	**BCR Members' employees** **Controller/Client's End customer / Prospects**
	WPS/ WKS related services	**Collection and Analysis of KYC Documents (on behalf of ordering clients)**	**1.Identification data** (e.g., Name, Last name) **2. KYC information** (e.g., go/no go, results of KYC investigations)	**Client/Controller's end customer / prospect**

Domain of processing activities		Purpose of processing	Categories of Personal Data	Categories of Data Subjects
		Client Applicants Background Checks / KYE (on behalf of ordering clients)	**1.Identification data** (e.g., Name, Last name) **2. KYC information** (e.g., go/no go, results of KYC investigations)	**Client/Controller's end customer / prospect**

DOCUMENT CONTROL

Version	Update	Modifications Summary
0.1	27/02/2022	Final Approval
0.2	19/05/2023	Document control (added) Update of countries and Regions
0.3	01/04/2024	Re-branding and formatting

Review Frequency	This document will be reviewed at least annually or upon change
Date of Issue	25/05/2018
Domain	Privacy
Classification	Public
Reference	BCR Appendix 11B