# MANUAL DE PRIVCIDAD Y PROTECCIÓN DE DATOS DE LATAM

# MANUAL DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

# PERDSONAL DATA AND PRIVACY MANUAL

# CONCENTRIX LATAM & THE CARIBBEAN

## INDICE

# 1. OBJETIVO

El grupo de sociedades comerciales que conforman el grupo Concentrix (en adelante conjuntamente denominadas como "Concentrix" y/o "CX"), reconocen la importancia de la seguridad, privacidad y confidencialidad de la información personal que los usuarios, clientes, proveedores, empleados, aliados comerciales, candidatos y terceros, pueden llegar a suministrar y/o transferir a Concentrix, a través de los diversos canales habilitados, tales como, pero son limitarse a: sitios web, aplicaciones, redes sociales, documentos físicos y/o digitales.

Como consecuencia de lo anterior, Concentrix está comprometida con: (i) la efectiva protección de los derechos de los Titulares[1]; y (ii) el adecuado Tratamiento[2] de los Datos Personales[3], conforme a la normativa aplicable en materia de privacidad y protección de datos personales.

Así pues, el objetivo del presente Manual Interno de Privacidad y Protección de Datos Personales (en adelante el "Manual"), es el de complementar las disposiciones generales de la Política de Tratamiento de Datos Personales para Concentrix en: https://www.concentrix.com/legal/ y definir los lineamientos internos generales aplicables a Concentrix para garantizar la aplicación, monitoreo, sostenimiento y mejora continua de los procedimientos asociados al Tratamiento de los datos personales en el desarrollo de sus actividades.

# 2. ALCANCE

El alcance del presente Manual es establecer: (i) el procedimiento para el manejo de los PQR´s relacionados con el tratamiento de los datos personales, que se llevarán a cabo a nivel interno, cuando Concentrix actúe como responsable de los datos personales; (ii) el procedimiento de recepción y escalamiento a nuestros clientes de los PQRs relacionados con el tratamiento de los datos personales, cuando Concentrix actúe como encargado de los datos personales, (en adelante "escalation"), y; (iii) el procedimiento interno ante la posible ocurrencia de un incidente de seguridad de la información o "data protection/privacy breach".

Este Manual aplica de manera vinculante y transversal a Concentrix LATAM y el Caribe, entendido como todas sus sociedades filiales y subsidiarias de CX en LATAM y el Caribe[4] ; las cuáles son descritas en el numeral 5 de la Política de Tratamiento de Datos Personales https://www.concentrix.com/legal/ Por lo tanto, su conocimiento y adecuada

[1] Cómo se define más adelante.
[2] Ibidem.
[3] Ibidem.
[4] CX está compuesta por las sociedades establecidas en los siguientes países: Estados Unidos (solo cuando el cliente se encuentre localizado en Latino América), México, El Salvador, Guatemala, Honduras, Nicaragua, Costa Rica, República Dominicana, Jamaica, Colombia, México, Perú, Panamá, El Salvador, Nicaragua, Guatemala, Honduras, entre otros..

aplicación son obligatorias para todos los gamechangers que hacen parte de CONCENTRIX LATAM.

d

## 3. DEFINICIONES

El presente Manual se rige por las siguientes definiciones:

3.1. **Administrador de las Bases de Datos:** Es la persona natural vinculada con Concentrix, a la que se le asigna como parte de sus funciones, bajo contrato laboral o de servicios, el desarrollo de tareas y responsabilidades inherentes a las Bases de Datos Personales de la Organización. El Administrador de las Bases de Datos es responsable de la vigilancia de la debida aplicación de las Políticas de Privacidad que sean aplicables respecto de cada proceso y de proveer al oficial de protección de datos personales y/o al área de Cumplimiento la información requerida para cumplir con todos los requisitos legales en la materia como el registro periódico de bases de datos y su actualización.

3.2. **Archivos o repositorios de información:** conjunto de documentos en medio físico o digital, conservados por la empresa en donde conste información personal regulada por la ley.

3.3. **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de los Datos Personales.

**Nota:** En la legislación de Brasil existen diversas bases legales que permiten el tratamiento de datos personales, las cuales incluyen, además de la autorización consentimiento del titular, otras 9 (nueve) posibilidades[5]

3.4. **Autoridad de Protección de Datos:** Es la autoridad encargada en cada país de vigilar y supervisar que en el Tratamiento de Datos Personales se respeten los principios, derechos y garantías de los Titulares.

3.5. **Aviso de Privacidad:** Es el documento físico, electrónico o en cualquier otro formato conocido o por conocer, que es puesto a disposición del Titular con el fin de informar sobre el Tratamiento de sus Datos Personales. En el aviso de Privacidad se comunica a los Titulares la información relativa a la existencia de las políticas de Tratamiento de información que serán aplicables, la forma de acceder a las mismas y las características del Tratamiento que se pretende dar a los Datos Personales.

3.6. **Base de Datos:** Conjunto organizado de Datos Personales que sea objeto de Tratamiento.

[5] Lo anterior de conformidad con el art. 7° de la Ley 13709/2018 – Ley General de Protección de Datos Personales de Brazil (LGPD)

3.7. **Causahabiente:** Persona que por sucesión o transmisión adquiere los derechos de otra persona.

3.8. **Colaborador Autorizado:** Colaborador de Concentrix que está autorizado por su labor o funciones específicas para acceder o dar cualquier tipo de tratamiento a una base de datos administrada por Concentrix, la cual puede contener datos personales.

3.9. **Comité de Protección de Datos Personales:** Órgano interno de Concentrix integrado por el gerente legal, el gerente de Cumplimiento, los delegados del área de Cumplimiento IT, los delegados del área de Seguridad de la información y el Oficial de Protección de Datos Personales, con el fin de velar por la implementación efectiva de políticas y procedimientos adoptados en cumplimiento del régimen general de protección de datos personales y ejecutar planes de acción en caso de posibles incidentes de seguridad de la información que puedan afectar la integridad, confidencialidad y/o integridad de los datos personales.

3.10. **Consulta:** Es la petición que hace el Titular sobre sus Datos Personales que reposan en las bases de datos de Concentrix y que no se encuentran restringidas de conformidad a la legislación, según los procedimientos establecidos en el Programa Integral de Gestión de Datos Personales

3.11. **Dato(s) Personal(es):** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

3.12. **Datos sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

3.13. **Oficial de Protección de Datos Personales y/o Delegado y/o Líder Local de Protección de Datos:** Es la persona natural que cumple con el perfil establecido por la ley y que tiene como función la vigilancia y control sobre la aplicación de la Política de Tratamiento de Datos Personales.

**Nota:** En la normativa aplicable en Brasil, la anterior definición corresponde al término de Encargado del tratamiento de los datos personales (Encarregado de Proteção de Dados)

3.14. **Escalation:** procedimiento de escalamiento de solicitudes de los titulares de la información a los clientes de Concentrix, para que estos le den respuesta directamente.

3.15. **Encargado / Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de Datos Personales por cuenta del Responsable del Tratamiento.

**Nota:** En la normativa aplicable en Brasil, la anterior definición corresponde al término de Operador.

3.16. **Habeas Data (cuando aplique):** Derecho que tiene toda persona de conocer, actualizar y rectificar la información que se haya recogido sobre ella en archivos y bancos de datos de naturaleza pública o privada.

3.17. **Incidente o evento de seguridad:** pérdida, acceso, uso no autorizado y/o robo de Datos Personales, violación a los procedimientos contenidos en este Manual y en las Políticas de Privacidad y de seguridad de la información de Concentrix, entrega no autorizada de información y Datos Personales a terceros, Tratamiento de Datos Personales no autorizado conforme las Políticas de Privacidad de Concentrix.

3.18. **Normas corporativas Vinculantes:** Constituye uno de los mecanismos legales establecidos por la ley que permite las transferencias de información dentro de un Grupo empresarial.

3.19. **PQRs:** Término que incluye Peticiones, Quejas, Reclamos y Sugerencias de los titulares de la información o que pretendan hacer valer derechos relativos a los datos personales.

3.20. **Reclamo:** Es la petición que hace el Titular sobre sus Datos Personales que reposan en las bases de datos de Concentrix, por medio del cual puede solicitar la supresión de sus datos personales y/o revocar la autorización otorgada para el Tratamiento de los mismos

3.21. **Responsable /Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

**Nota:** En la normativa aplicable en Brasil, la anterior definición corresponde al término: Responsable

3.22. **SubEncargado:** empresa contratada por el encargado/Encargado para el procesamiento de datos personales.

3.23. **Titular(es):** Persona natural cuyos Datos Personales sean objeto de Tratamiento.

3.24. **Transferencia de Datos Personales o de Bases de Datos Personales:** Es la entrega de Datos Personales o de Bases de Datos Personales por parte de un Responsable del Tratamiento de Datos Personales a otra persona natural o jurídica

para que ésta última actúe en su propio nombre como Responsable del Tratamiento de los Datos Personales o de las Bases de Datos recibidos.

3.25. **Transmisión de Datos Personales:** Es la entrega de Datos Personales o de Bases de Datos Personales por parte de un Responsable del Tratamiento a otra persona natural o jurídica para que ésta última, en su calidad de Encargada, realice el Tratamiento de Datos Personales por cuenta del que los entrega conforme a las obligaciones establecidas en el contrato que para el efecto se celebre.

3.26. **Tratamiento:** Cualquier operación o conjunto de operaciones sobre Datos Personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

3.27. **Incidente de seguridad de Datos Personales:** Toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de los Datos Personales conservados o tratados, o la comunicación o acceso no autorizado a dichos datos.

3.28. **Titulares de la Información:** Clientes, Proveedores, Subcontratistas, Visitantes, Colaboradores o Empleados de Concentrix, que hayan suministrado la información o Datos Personales en virtud del servicio prestado por este.

# 4. CONSIDERACIONES PREVIAS

## 4.1 Recolección de datos personales y consentimiento del titular

El Colaborador Autorizado para la recolección de los datos personales deberá solicitar y guardar constancia en un medio seguro de la autorización de tratamiento de datos personales del titular de la información, salvo que la ley aplicable en materia de tratamiento de datos personales disponga que esta no se requiere.

De forma previa a realizar cualquier tipo de Tratamiento de Datos Personales (captura o recolección, uso, almacenamiento, circulación, transmisión, transferencia, actualización, modificación, supresión, entre otros), el Colaborador Autorizado para ello debe verificar que los datos personales que van a ser suministrados sean los estrictamente necesarios para cumplir con las finalidades para los cuales se requieren y que están establecidas en la Política de Privacidad de Concentrix.

El Colaborador Autorizado no podrá hacer Tratamiento de Datos Personales de manera aislada, en documentos o manuscritos que no formen parte de la Base de Datos respectiva, la cual será reportada al área de Cumplimiento y al oficial de protección de datos personales.

Cuando la recolección de la información se haga a través de medios no presenciales, tales como la página web, aplicación móvil y/o Call center, la evidencia de la autorización para la Recolección y Tratamiento del Dato Personal por parte del Titular, constará en el sistema utilizado por el medio no presencial (Ejemplo: en página web y aplicación móvil, la constancia se genera al dar clic en la casilla “Aceptar” de los check-box, al aceptan las Políticas de privacidad; así mismo, en el Call Center la prueba de la autorización se puede conservar en la grabación de la llamada).

Si no es posible poner a disposición de los Titulares de la información las Políticas de Privacidad y las finalidades del tratamiento, se deben fijar Avisos de Privacidad en lugares visibles y de fácil acceso, de manera física o digital, en los lugares físicos o sitios web donde se realice la recolección de datos personales.

## 4.2 Creación y/o modificación de Bases de Datos

Concentrix cuenta con unas Bases de Datos previamente identificadas por el área de gobierno de datos, cuyo control está en cabeza de los administradores de Bases de Datos Personales dentro de la Organización, este proceso debe tener apoyo y orientación del área de Cumplimiento y al oficial de protección de Datos Personales.

Siempre que se lleve a cabo la creación de una nueva base de datos, así como la modificación a las Bases de Datos Personales ya existentes, se deberá contar con el visto bueno del área de gobierno de datos y el área y/o delegado dentro de la organización para la Protección de Datos Personales a través de la solicitud de autorización remitida al correo

electrónico: proteccion.dedatos@concentrix.com y protección.dedatos@Concentrix.com con el fin de llevar la trazabilidad de los repositorios de información y bases de datos y hacer el reporte correspondiente a las autoridades de protección de datos personales cuando esto aplique.

## 4.3 Adecuado almacenamiento de Datos Personales

- Independientemente del medio de recolección de los datos personales, ya sea físico o digital, se deberá solicitar y conservar en adecuadas condiciones de seguridad el correspondiente consentimiento del titular de los datos, y de acuerdo con los parámetros establecidos en la Política de Tratamiento de Datos Personales de Concentrix.

- Los Datos Personales deben ser almacenados en Bases de Datos o repositorios de información que cumplan con las medidas de seguridad definidas en la Política de Seguridad de la Información disponible para consulta en la plataforma de gestión documental Isolución como: SI-T-R-S-006 SEGURIDAD DE LA INFORMACION.

- Las Bases de Datos físicas, deben cumplir con medidas de seguridad adecuadas con el fin de evitar la consulta sin autorización, alteración y/o perdida de la información personal

- Para el tratamiento de los documentos que contengan datos personales se debe cumplir con los lineamientos y procedimientos en materia de gestión documental de Concentrix.

## 4.4 Circulación de los Datos Personales

- Los Colaboradores y/o terceros vinculados podrán compartir con otros Colaboradores, terceros vinculados autorizados y/o áreas de la Organización los Datos Personales cuando esto sea necesario para el cumplimiento de sus funciones, de acuerdo con las responsabilidades de su cargo. Sin embargo, este Tratamiento de información personal debe realizarse en estricto cumplimiento de las finalidades del tratamiento de la información recolectada y de conformidad con lo establecido en las Políticas de Privacidad de Concentrix.

- Está prohibido y se considera falta grave que los Colaboradores y/o terceros vinculados circulen, transfieran, transmitan, envíen, compartan y/o comuniquen información personal de Titulares de la información a colaboradores que no estén autorizados para acceder a esta o a terceros ajenos a Concentrix. Si un colaborador conoce de una posible fuga de información deberá comunicarse con la línea ética y poner en conocimiento del área de Cumplimiento y del oficial de protección de datos personales.

- Cuando un colaborador reciba una solicitud que involucre la entrega de datos personales, ya sea por parte de una Autoridad o de un particular, esta deberá ser canalizada al área de Cumplimiento y/o al oficial de Protección de Datos Personales con el fin de evaluarla y otorgar respuesta de acuerdo con el procedimiento descrito en los numerales 4 a 6 del presente Manual.

- Ante cualquier duda o consulta sobre el uso y circulación de Datos Personales en relación con la finalidad para la cual fueron recolectados, o sobre el tratamiento de datos personales en general, los colaboradores podrán acudir al área de Cumplimiento o al oficial de protección de datos personales.

## 4.5 Transferencia y Transmisión de los Datos Personales recolectados

Concentrix podrá Transferir (de Responsable a Responsable) o Transmitir (de Responsable a Encargado) los Datos Personales que se encuentren en las bases de datos de la Organización, siempre y cuando se le informe al Titular de esa finalidad y se cumpla con las salvaguardas establecidas en la ley aplicable para la Transferencia y/o Transmisión de Datos Personales. Si la Transmisión se realiza a terceros ubicados en diferentes países, se deberá celebrar un contrato de transmisión internacional de datos personales con ese Encargado o se aplicará la salvaguarda jurídica que aplique, según el caso.

## 4.6 Tratamiento de Datos Personales de Niños, Niñas y Adolescentes

El Tratamiento de Datos Personales de niños, niñas y adolescentes, se realizará excepcionalmente, teniendo en cuenta las finalidades del tratamiento de los datos, el respeto de sus derechos fundamentales y su interés superior y su derecho a ser escuchado previamente. Así mismo, se requerirá la autorización de quien tenga su patria potestad o su representante legal

El Colaborador y/o tercero encargado que a razón de sus funciones tenga conocimiento de Datos Personales de niños, niñas y adolescentes, debe tener especial protección y el Tratamiento de estos datos exige la implementación de mayores medidas de seguridad y cuidado.

## 4.7 Tratamiento de Datos Sensibles

El colaborador y/o tercero encargado que en razón a sus funciones deba realizar Tratamiento de datos sensibles debe tener una diligencia mayor para salvaguardar su integridad, confidencialidad y seguridad. Por lo tanto, solo se podrá realizar el Tratamiento de los Datos sensibles cuando la ley aplicable así lo permita y con la autorización expresa del titular de la información, salvo las excepciones de ley.

# 5. BUENAS PRÁCTICAS PARA DAR RESPUESTA A REQUERIMIENTOS Y PQRs

Para efectos de dar trámite a cualquier requerimiento o PQR, se debe seguir los siguientes pasos:

5.1. Identificar el objeto del Requerimiento para dar a este una respuesta directa, clara y concreta Cuando se realice la generación de nuevas Bases de Datos que contengan Datos Personales el área encargada deberá garantizar el cumplimiento de lo dispuesto en las Políticas y Procedimientos de seguridad de la información y de gestión documental de Concentrix.

5.2. Mencionar los hechos que permitan entender de forma lógica las respuestas.

5.3 Hacer referencia precisa a documentos que se envíen o entreguen como anexos, de tal forma que exista un nexo causal entre el Requerimiento y las respuestas.

5.3. Exponer de forma concreta, las justificaciones legales, técnicas y/o contractuales, que sean aplicables o necesarias.

5.4. Cuando existan situaciones susceptibles de ser mejoradas y/o corregidas, informar las medidas que se estén estudiando o que serán adoptadas

5.5. Velar por que la respuesta no cause reprocesos o reiteraciones por parte de la Autoridad Competente o por parte del titular

5.6. Relacionar, al final de cada contestación, los anexos o archivos correspondientes, indicando brevemente el propósito de estos y con la enunciación de su contenido o denominación, debidamente foliados.

5.7. Abstenerse de enviar información y documentos que no sean solicitados o que no estén relacionados directamente con el Requerimiento.

5.8. Documentar la respuesta a todo Requerimiento (sea verbal, física o electrónico), a través del respectivo radicado

5.9. Mantener en un lugar seguro una copia de la respuesta al Requerimiento y de sus respectivos anexos.

5.10. Cuando los Requerimientos del titular o de las Autoridades Competentes no sean claros o contengan imprecisiones formales que puedan incidir en la respuesta, contactar con suficiente antelación al vencimiento, a la Autoridad Competente, con el fin de precisar los puntos en cuestión, sin sobrepasar el tiempo máximo legal para dar respuesta al requerimiento

# 6. PROCEDIMIENTO PARA EL MANEJO DE REQUERIMIENTOS DE AUTORIDADES COMPETENTES

Los Colaboradores encargados de la recepción, respuesta y envío de los requerimientos deberán seguir el siguiente procedimiento para dar respuesta a requerimientos de autoridades competentes, sin perjuicio del tipo de Requerimiento:

## 6.1. Recepción del Requerimiento de autoridad competente o PQR

En el evento que un colaborador de Concentrix reciba un Requerimiento relacionado con datos personales o solicitando algún tipo de datos personales a través de cualquier canal de recepción, este, dentro de un plazo no mayor a un (1) día hábil, deberá comunicarlo y notificarlo, según corresponda al correo electrónico: protección.dedatos@concentrix y/o proteccion.dedatos@concentrix.com, al oficial de protección de datos personales /área de Cumplimiento y a su superior inmediato.

Incumplir con este deber, se podrá entender como una falta grave.

## 6.2. Envío del requerimiento al área responsable

Una vez recibido el Requerimiento, el área o dependencia asignada por Concentrix para dicha recepción deberá establecer e identificar el tipo de solicitud y su objeto, con el fin de direccionarla al área responsable de darle respuesta.

Con el fin de determinar el área o departamento de Concentrix que debe dar respuesta al Requerimiento, se deberá tener en cuenta los siguientes criterios:

| Tipo de Requerimiento | Área o Departamento Responsable de Contestar el Requerimiento | Dato de Contacto |
|---|---|---|
| Requerimientos relacionados con prevención, investigación y sanción de actos de corrupción. | Departamento de Cumplimiento | E-mail: natalia.lewis@concentrix.com |
| Requerimientos relacionados con riesgos Laborales y salud ocupacional | Departamento de Recursos Humanos | E-mail: relaciones.laborales.co@onelinkbpo.com |
| Requerimientos relacionados con el manejo de datos personales | Departamento de Privacidad / Datos Personales | E-mail: proteccion.dedatos@concentrix.com |
| Requerimientos relacionados con temas de competencia desleal, prácticas | Departamento Legal | E-mail: juliancamilo.diaz@concentrix.com |

| | | |
|---|---|---|
| restrictivas y propiedad intelectual. | | |
| Requerimientos relacionados con temas de comercio electrónico y protección al consumidor | Departamento Legal | E-mail: juliancamilo.diaz@concentrix.com |

## 6.3 Determinar si Concentrix es competente

En caso de que Concentrix no sea competente, por no ser el sujeto indicado para dar respuesta al Requerimiento, deberá informarlo de inmediato a la Autoridad Competente, si este actúa verbalmente, o dentro de los dos (2) días hábiles siguientes al recibo, en caso de que el Requerimiento se haya recibido por escrito o electrónicamente.

## 6.4 Determinar si la solicitud está completa o se debe requerir información adicional o soportes

En caso de que la solicitud no sea clara o resulte incompleta, se solicitará aclaración a la autoridad solicitante tan pronto como sea posible y dentro de un máximo de los dos (2) días hábiles siguientes la fecha de su recepción, y una vez se reciba la información requerida se procederá de forma inmediata a dar respuesta al requerimiento, para así dar cumplimiento dentro del término establecido por la autoridad competente.

## 6.5 Establecer si el Requerimiento involucra datos personales o información reservada o confidencial de Concentrix

Cuando el Requerimiento implique revelar o suministrar información reservada o confidencial, Concentrix deberá indicarlo a la Autoridad Competente en la respuesta al Requerimiento.

Asimismo, cuando se trate de datos personales de titulares de la información, que sean objeto de tratamiento de Concentrix, una vez elaborado por el área encargada de otorgar la información, el requerimiento deberá ser revisado por el área de Cumplimiento y por el oficial de protección de datos personales de Concentrix para aprobar la respuesta y verificar que cumpla con los requisitos de la normativa en tratamiento de los datos personales.

Por titulares de la información se entienden aquellas personas naturales o jurídicas, que son contratistas, clientes, proveedores o aliados comerciales de Concentrix, de los cuales se trata información confidencial o reservada, que puede verse ser solicitada en un Requerimiento.

## 6.6 Elaboración de la respuesta al requerimiento

La respuesta al requerimiento se realizará por el área de Concentrix encargada de otorgar la información requerida. La respuesta deberá cumplir con los siguientes requisitos: i) oportuna, ii) objetiva, iii) veraz, iv) completa, v) motivada y vi) actualizada.

- Es oportuna cuando se radica en los plazos estipulados por la ley o en el Requerimiento.

- Es objetiva cuando se responde con base en el contenido de los documentos y pruebas que se adjuntan.

- Es veraz cuando su contenido es verificable de acuerdo con los documentos y pruebas que se adjuntan.

- Es completa cuando se responde cada uno de los interrogantes y/o solicitudes del Requerimiento.

- Es motivada cuando existe justificación frente a las diferentes disposiciones que se incluyan en la contestación al Requerimiento.

- Es actualizada cuando se fundamente en información y datos recientes.

- En los casos en que los Requerimientos tengan diferentes solicitudes o cuestionamientos, estos deberán contestarse en el mismo orden en que se solicitan y de forma clara

## 6.7 Envío de la respuesta

- Independientemente del medio en que haya sido recibido el Requerimiento, la respuesta se enviará por medio escrito, ya sea por medio electrónico (como correo electrónico) o físico, de acuerdo a lo indicado por la Autoridad Competente

- La respuesta al Requerimiento deberá ser enviada a la dirección fisica o electrónica enunciada en el requerimiento o en los medios oficiales de la autoridad que hizo el requerimiento

- La respuesta al Requerimiento deberá dirigirse a la Autoridad Competente y al funcionario que realizó el requerimiento

- Para efectos de probar el envío, se deberá conservar el comprobante y el número de radicado del Requerimiento.

## 6.8 Término para dar respuesta al Requerimiento de autoridad competente

Salvo norma o disposición especial, los Requerimientos deberán resolverse dentro del plazo enunciado en el requerimiento. Cuando excepcionalmente no sea posible resolver el Requerimiento en el plazo anteriormente señalado, Concentrix, a través del área o dependencia competente encargada de dar respuesta y/o a la que fue direccionada el Requerimiento, deberá informar de dicha circunstancia a la Autoridad Competente, expresando los motivos del retraso y señalando el plazo razonable en que se resolverá o dará respuesta.

# 7. PROCEDIMIENTO PARA DAR RESPUESTA A PQRs DE LOS TITULARES DE LA INFORMACIÓN

Este procedimiento solo aplica cuando Concentrix actúe en su calidad de Responsable del tratamiento de los datos personales, ya que cuando actúe como encargado, por regla general se deberá seguir el procedimiento de "Escalation" previamente establecido con el cliente para transferirle los PQRs y que este les dé respuesta directamente.

## 7.1. Cuando Concentrix es responsable de los datos personales

Los usuarios, clientes, proveedores, empleados o postulantes de Concentrix tienen derecho a conocer los detalles del tratamiento de sus datos personales y a ejercer los derechos que les asisten como Titulares de estos, por medio de consultas, solicitudes y quejas en los términos de las normas de protección de datos que les sean aplicables y conforme lo establecido en la presente Política de Privacidad.

Para efectos de lo anterior, el presente Manual define el procedimiento general para el ejercicio de los derechos por parte de los Titulares de la información, sin perjuicio de la aplicación de procedimientos y requerimientos específicos que las leyes locales de cada territorio puedan contemplar. En caso de discrepancia entre el procedimiento general establecido en este Manual y los procedimientos o requerimientos específicos contenidas en las normas locales aplicables de cada territorio, primarán estas últimas.

### 7.1.1 Recepción de PQR'S (CORREO, VENTANILLA, FAX Y/O E-MAIL).

las solicitudes se podrán presentar por medio escrito, físico y/o digital, y a través de los canales habilitados por la Organización para ello, que son:

i) Presencialmente, ya sea verbal o por escrito, en los espacios físicos que destine Concentrix para dichos efectos, tales como las oficinas ubicadas en: Calle 63 # 24 – 80, en Bogotá - Colombia

ii) Telefónicamente, al número teléfono: (+57) 4 444 38 20

iii) Al correo físico o postal, que según el país correspondiente será:

Al correo electrónico: proteccion.dedatos@concentrix.com y/o protección.dedatos@Concentrix.com

En el evento que un colaborador de Concentrix reciba un Requerimiento relacionado con datos personales a través de canales de recepción distintos a los que se mencionan en este numeral, este, dentro de un plazo no mayor a un (1) día hábil, deberá comunicarlo y notificarlo, según corresponda, al siguiente correo electrónico: al oficial de protección de datos personales /área de Cumplimiento y a su superior inmediato.

Incumplir con este deber, se podrá entender como una falta grave.

### 7.1.2. Determinar si Concentrix es competente

Una vez recibido el Requerimiento, el área de Cumplimiento o el Oficial de Protección de Datos Personales determinará si Concentrix es competente para resolver la solicitud

En caso de que Concentrix no sea competente deberá informarlo al titular o interesado dentro de los dos (2) días hábiles siguientes al recibo (salvo pacto en contrario que establezca un término diferente en el contrato o en otro documento suscrito con el cliente).

### 7.1.3 Determinar si el solicitante está legitimado para realizar la solicitud

Es fundamental determinar si el consultante está legitimado para realizar la solicitud; esto dependerá de la legislación aplicable pero por regla general el solicitante deberá ser: i) el titular de los datos o ii) su representante legal, o iii) una persona debidamente autorizada por el titular para hacer la consulta o reclamo o iv) su heredero legal dado que el entregar información personal, modificarla o suprimirla cuando no se trate de la persona legitimada por la ley para ello puede resultar en una violación de la protección de los datos personales y perjudicar negativamente a Concentrix. Por lo tanto, se debe tener en cuenta lo siguiente:

- El Titular de la información y/o quien ejerce el derecho en su nombre, debe acreditar su Titularidad con el fin de evitar la pérdida, consulta, uso o acceso no autorizado o fraudulento por una persona distinta del Interesado y/o que no tenga mandato legal para actuar en nombre de este.

- La acreditación por parte del Titular se surtirá mediante el envió de: copia física o digital del documento de identificación pertinente de acuerdo con el medio de presentación de la consulta.

- Cuando la petición sea formulada por persona distinta al Titular, el tercero deberá acreditar en debida forma la personería o mandato para actuar en nombre de este enviando los documentos que lo soporten.

La petición se gestionará por el área y/o delegado encargado dentro de la organización para la protección de datos personales únicamente cuando se pueda acreditar la Titularidad y se cumpla con los requisitos anteriormente nombrados.

### 7.1.4 Determinar si la solicitud está completa o se debe requerir información adicional o soportes

La solicitud del ejercicio de cualquiera de los derechos mencionados debe contener como mínimo la siguiente información:

- Nombre del Interesado, de su representante y/o la persona que ejerce el derecho en su nombre, y número de identificación.
- Petición concreta, precisa y justificada de la consulta y del derecho invocado.
- Dirección física y/o electrónica para notificaciones.
- Documentos que soportan la solicitud (si aplica)
- Firma del peticionario de acuerdo con el medio de la solicitud.

Si la solicitud resulta incompleta, se requerirá al interesado dentro de los cinco (5) días hábiles siguientes la fecha de su recepción, para que subsane las fallas.

La información requerida debe ser presentada por el solicitante dentro de los dos (2) meses siguientes al requerimiento; si no lo hace se entenderá que ha desistido.

La petición se gestionará por el área y/o delegado encargado dentro de la organización para la protección de datos personales únicamente cuando se pueda acreditar la Titularidad y se cumpla con los requisitos anteriormente nombrados.

### 7.1.5 Redireccionamiento de la solicitud

Si se determina que Concentrix es competente para dar respuesta, se procederá a determinar si la solicitud es de carácter técnico o legal o tiene una parte técnica y otra legal, con el fin de direccionarla al área responsable de darle respuesta.

Si la solicitud es enteramente de carácter legal procederá a resolverla directamente el área de Cumplimiento o el Oficial de Protección de Datos Personales; de lo contrario solicitará apoyo al área de Seguridad de la Información y/o al área encargada de dar respuesta a la solicitud.

### 7.1.6 Elaboración de la respuesta al requerimiento

La respuesta al requerimiento deberá ser oportuna, objetiva, veraz, completa, motivada y actualizada.

- Es oportuna cuando se radica en los plazos estipulados por la ley o en el Requerimiento.
- Es objetiva cuando se responde con base en el contenido de los documentos y pruebas que se adjuntan.
- Es veraz cuando su contenido es verificable de acuerdo con los documentos y pruebas que se adjuntan.
- Es completa cuando se responde cada uno de los interrogantes y/o solicitudes del Requerimiento.
- Es motivada cuando existe justificación frente a las diferentes disposiciones que se incluyan en la contestación al Requerimiento.
- Es actualizada cuando se fundamente en información y datos recientes.
- En los casos en que los Requerimientos tengan diferentes solicitudes o cuestionamientos, estos deberán contestarse en el mismo orden en que se solicitan y de forma clara.

### 7.1.7 Envío de la respuesta

- Independientemente del medio en que haya sido recibido el Requerimiento, la respuesta se enviará por medio escrito, ya sea por medio electrónico (como correo electrónico) o físico, de acuerdo a lo indicado por la Autoridad Competente
- La respuesta al Requerimiento deberá ser enviada a la dirección física o electrónica señalada por el titular de la información o el solicitante interesado
- La respuesta al Requerimiento deberá dirigirse al solicitante que realizó el requerimiento

- Para efectos de probar el envío, se deberá conservar el comprobante y el número de radicado del Requerimiento.

### 7.1.8 Término para dar respuesta a PQRs de los titulares de datos personales

El término máximo con el que cuenta Concentrix para atender la solicitud, es de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender la solicitud dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su solicitud, la cual no podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

## 7.2 Cuando Concentrix es encargado de los datos personales (Escalation)

Cuando Concentrix recibe PQR´s de titulares y frente a sus datos personales y actúa únicamente como encargado de la información, este remite al responsable de la información las solicitudes que recibe mediante el procedimiento de Escalamiento o Escalation, para que el cliente pueda dar respuesta directa a los peticionarios /titulares de la información.

El procedimiento de Escalation y los datos de contacto para escalar las solicitudes y peticiones de los titulares de la información se deberán acordar previamente y describirse en los acuerdos que Concentrix suscribe con el cliente al momento de iniciar su relación contractual.

- Elaborar un guion de escalamiento para el tratamiento de datos personales en el cual se incluyan las directrices generales de como direccionar un PQR en los canales disponibles del responsable para el tratamiento de los datos personales.

- Solicitar aprobación del responsable de tratamiento de datos personales sobre el guion de escalamiento.

- Socializar el guion de escalamiento con áreas de entrenamiento operativo para su implementación.

# 8. MEDIDAS DE SEGURIDAD E INCIDENTES DE SEGURIDAD

## 8.1 Medidas de Seguridad

Concentrix tiene definidas e implementadas las medidas de seguridad pertinentes para la protección de la información Personal de todos nuestros clientes, colaboradores, proveedores y accionistas, las cuales se han establecido basándose en estándares y regulaciones internacionales, tales como ISO27001:2013, PCI-DSS (Estándar de Seguridad para la información de Tarjetas de Crédito) y SOX (Ley Sarbanes-Oxley).

Las medidas de seguridad se encuentran establecidas en la Política de Seguridad de la Información, así como en las Políticas y Procedimientos Específicos y Estándares de Seguridad citados a continuación:

- Política de Seguridad de la Información
- Política de Gestión de Incidentes
- Política de Criptografía
- Política de Gestión de Activos de Información
- Política de Gestión de Accesos
- Política de Seguridad en las Operaciones

## 8.2 Eventos de incumplimiento de las Políticas de Privacidad, Política de Seguridad de la Información y Normas aplicables

En caso de presentarse un posible Incidente de Seguridad referente al Tratamiento de Datos Personales, este deberá ser reportado al área y/o delegado dentro de la Organización para la Protección de Datos Personales al correo electrónico: proteccion.dedatos@concentrix.com por el colaborador o colaboradores que hayan tenido conocimiento del mismo, de manera inmediata a su ocurrencia, con el fin de dar inicio a la investigación pertinente, al plan de acción y medidas correctivas, y se realice el reporte respectivo a las áreas internas y autoridades competentes, dentro de los términos establecidos por la Ley, en caso de proceder.

# 9. RESPONSABILIDAD DEL TRATAMIENTO DE LAS BASES DE DATOS DE CONCENTRIX

Cada una de las áreas y colaboradores que administran datos personales en el ejercicio de sus labores son responsables del adecuado manejo de las bases de datos y demás repositorios de información que contengan datos personales, y de cumplir con las políticas y procedimientos de Concentrix en materia de Tratamiento de datos personales, seguridad de la información y gestión documental. Así mismo, tienen el deber de entregar oportunamente y de forma completa la información requerida por el área de Cumplimiento y/o el oficial de protección de datos personales y colaborar con estas áreas para facilitar el cumplimiento de los requerimientos legales en la materia.

# 10. SANCIONES POR INCUMPLIMIENTO EN EL TRATAMIENTO DE DATOS PERSONALES

## 10.1 Sanciones a Concentrix

Las sanciones que podrán ser impuestas por las autoridades competentes a los Colaboradores y a Concentrix varían dependiendo de la normativa aplicable según el país o

países en que se incumpla con las Obligaciones de Protección de Datos Personales, las cuales podrán consistir, sin limitarse a:

- Multas de carácter Personal e Institucional que podrán ser sucesivas mientras subsista el incumplimiento que las originó.

- Suspensión de las actividades relacionadas con el Tratamiento de Datos Personales. En el acto de suspensión se indicarán los correctivos que se deberán adoptar.

- Cierre temporal de las operaciones relacionadas con el Tratamiento de Datos Personales una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la autoridad competente.

- Cierre inmediato y definitivo de la operación que involucre el Tratamiento de Datos Sensibles.

## 10.2 Sanciones a los colaboradores

En caso de incumplimiento a las políticas y procedimientos de Protección de Datos Personales establecidos en este Manual, Concentrix contempla sanciones administrativas para todos los colaboradores, las cuales, de acuerdo con su responsabilidad en el hecho y la gravedad del incumplimiento pueden conllevar hasta la terminación del vínculo contractual. Así mismo, el Comité de Ética, en aras de asegurar el cumplimiento del Código de Ética y Normas de Conducta de CNX, tiene la función de conocer, analizar, evaluar, tramitar, decidir y notificar las infracciones, quejas y denuncias referentes a la protección de los datos personales.

Los colaboradores que tengan acceso a información personal en razón de sus funciones en Concentrix se obligan a no difundir, comentar, copiar, entregar, comunicar, dar acceso, intercambiar o comercializar de ninguna forma ni por ningún medio su usuario y/o contraseña y/o demás credenciales de acceso a los sistemas y plataformas, ya sean de Concentrix, del cliente, o de terceros, que se hayan puesto a su disposición, así como cualquier información de carácter personal de clientes, consumidores finales, empleados, compañeros de trabajo, y cualquier otro dato personal que reciba o conozca con ocasión o para el desempeño de sus funciones. Así mismo, tienen el deber de adoptar las medidas adecuadas de seguridad y de comunicar de forma inmediata de cualquier sustracción, alteración o pérdida de sus credenciales, de información confidencial o datos personales, de forma inmediata cuando tengan conocimiento de ello. El incumplimiento a esta obligación legal y contractual acarreará sanciones disciplinarias, civiles y/o penales, según corresponda.

## 11. RESPONSABLES DE PROTECCIÓN DE DATOS DE LA REGIÓN DE LATAM


## 12. USO DE INTELUGENCIA ARTIFICIAL Y DATOS PERSONALES

Concentrix, comprometido con la evolución tecnológica para mejorar los servicios los servicios de nuestros clientes y la experiencia de nuestros empleados, accionistas, usuarios y en general cualquier titular de la información, ha adoptado el desarrollo y uso de tecnologías de Inteligencia Artificial bajo la declaración de uso ético y de principio frente a la inteligencia artificial de Concentrix: https://www.concentrix.com/wp-content/uploads/2024/04/Concentrix-Generative-AI-Statement.pdf.

Por tanto, Concentrix en la implementación y desarrollo de tecnología de IA tendrá en cuenta declaración de principios para la protección de los datos personales procesados. Igualmente, tendrá como principios rectores: (i) La Privacidad desde el Diseño y por Defecto; (ii) Principio de Minimización de Datos Personales, y; (iii) Las obligaciones

impuestas por las normativas vigentes en materia de Inteligencia Artificial donde tengamos presencial comercial.

Concentrix se encuentra comprometido con el uso responsable y ético de cualquier avance tecnológico, en especial en relación con la protección integral de los datos personales sobre los cuales somos responsables y/encargados.

## 13 NORMAS CORPORATIVAS VINCULANTES – REMISIÓN AL MANUAL DE PROTECCIÓN DE DATOS DE CONCENTRIX.

Las Normas corporativas vinculantes o Binding Corporate Rules ("NCR" y/o "BCR"), en materia de protección de datos, son de obligatorio cumplimiento para el grupo empresarial Concentrix cuando las empresas que las componen al grupo realicen transferencia, o conjunto de transferencias, de datos personales a otro encargado dentro de una jurisdicción donde opere Concentrix, o bien, a otro país donde también opere la compañía.

Para el efecto, Concentrix en cumplimiento de la normativa de protección de datos personales de las jurisdicciones donde tiene presencia en Latino américa y el caribe, ha implementado un compendio de Normas Corporativas Vinculantes en materia de protección de datos personales las cuales fueron incluidas en nuestro Manual de Normas Corporativas Vinculantes, el cual podrán encontrar en: https://www.concentrix.com/legal/ en la sección de GEO Level Policies y subsección de LATAM.

Dentro de nuestro Manual podrá encontrar la totalidad de las BCR de Concentrix aplicable a la transferencia de datos personales y otros aspectos relativos a la privacidad.

## 14. ACUERDO GENERAL DE PROTECCION DE DATOS PARA CONTRATISTAS.

En virtud de los requerimientos normativos en materia de protección de datos personales de las jurisdicciones en las cuáles tenemos presencia comercial, y el interés del Grupo Concentrix de generar confianza a nuestros titulares sobre las medidas contractuales establecidas para proteger sus datos personales, hemos elaborado un Acuerdo General de Protección de Datos para Contratistas de Concentrix, el cual establece de forma estándar las medidas contractuales, organizativas, administrativas, humanas y técnicas que los Contratistas, que prestan servicios donde se ven incurso el tratamiento de datos de personal y/o accionistas, deben cumplir para prestar servicios a Concentrix.

De esta manera, cada Contratista, al diligenciar y firmar los formatos de proveedores, órdenes de servicios, órdenes de compra, carta de aceptación, carta oferta y algún documento vinculante comercial entre Concentrix y el Contratista, acepta, de forma expresa y univoca, el contenido del Acuerdo General de Protección de Datos para Contratistas el cual será el anexo 1 del presente Manual tanto en español, portugués e inglés.

# ANEXO 1. ACUERDO GENERAL DE PROTECCIÓN DE DATOS PERSONALES PARA CONTRATISTAS.

## a. Español

Este Acuerdo de Protección de Datos ('Acuerdo') se realiza como una enmienda a la relación contractual existente entre CONCENTRIX (Encargado de Datos) incluyendo sus empresas afiliadas y CUALQUIER PROVEEDOR QUE PROPORCIONE BIENES Y/O SERVICIOS en los que se procesen datos personales, referidos conjuntamente como las 'Partes'.

**CON LA ACEPTACIÓN DE LA ORDEN DE SERVICIO Y/O ORDEN DE COMPRA, EL PROVEEDOR RECONOCE Y ACEPTA LOS TÉRMINOS Y CONDICIONES CONTENIDOS EN ESTE DOCUMENTO LEGAL VINCULANTE.**

Fecha de Vigencia:

Fecha de vigencia de la aceptación de la orden de compra y/o orden de servicio o aceptación expresa de nuestros Manuales de Políticas y/o Reglas Corporativas Vinculantes o cualquier otro documento legal vinculante entre las partes.

### OBJETO

Este Acuerdo describe las responsabilidades y obligaciones del Encargado con respecto al procesamiento de datos personales en nombre del Responsable, garantizando el cumplimiento de la legislación de protección de datos en toda América Latina. Esto incluye, pero no se limita a, las diversas leyes y regulaciones nacionales de protección de datos en cada país de la región. El Encargado estará sujeto a la Política de Privacidad de Concentrix para Latam y al Manual de Privacidad de Datos y Reglas Corporativas Vinculantes para el Caribe. La documentación se puede encontrar aquí: El Encargado se compromete a ayudar al Responsable a obtener y mantener el consentimiento necesario de los sujetos de datos para el procesamiento de sus datos personales. Esto incluye garantizar que los sujetos de datos estén adecuadamente informados sobre los propósitos del procesamiento de datos, sus derechos bajo las leyes de protección de datos aplicables y cualquier otra información necesaria para asegurar el consentimiento informado.

### DEFINTICIONES

- **Datos Personales:** Cualquier información relacionada con una persona natural identificada o identificable.

- **Datos Personales Sensibles:** Datos personales que revelan el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos con el fin de identificar de forma única a una persona natural, datos sobre salud o datos sobre la vida sexual o la orientación sexual de una persona natural.

- **Datos Públicos:** Información que se pone a disposición del público de manera legal a partir de registros gubernamentales federales, estatales o locales, o de otras fuentes accesibles al público.

- **Datos Privados:** Datos personales que no están disponibles públicamente e incluyen información como nombres, direcciones, números de seguridad social y otros identificadores.

- **Datos Financieros:** Datos personales relacionados con el estado financiero de un individuo, incluidos, entre otros, detalles de cuentas bancarias, información de tarjetas de crédito, estados financieros e información de ingresos.

- **Procesamiento:** Cualquier operación o conjunto de operaciones que se realicen sobre datos personales o sobre conjuntos de datos personales, ya sea por medios automatizados.

- **Titulares:** Un individuo cuyos datos personales son procesados.

- **Responsable:** La entidad que determina los propósitos y medios del procesamiento de datos personales.

- **Encargado:** La entidad que procesa datos personales en nombre del Responsable.

- **Consentimiento:** Cualquier indicación específica, informada y no ambigua de los deseos del sujeto de datos mediante la cual, mediante una declaración o acción afirmativa clara, manifiesta su acuerdo para el procesamiento de datos personales que los concierne.

## ALCANCE Y APLICACIÓN

Este Acuerdo se aplica a todos los datos personales procesados por el Encargado en nombre del Responsable, incluidos datos privados, datos públicos, datos sensibles e información financiera. Este Acuerdo sirve como una enmienda al contrato existente entre el Responsable y el Encargado, incorporando los requisitos de protección de datos estipulados por la legislación relevante en toda América Latina.

## CUMPLIMIENTO DE LAS LEYES DE PROTECCIÓN DE DATOS

- Brasil: Ley General de Protección de Datos (LGPD)
- Argentina: Ley de Protección de los Datos Personales
- México: Ley Federal de Protección de Datos Personales en Posesión de los Particulares
- Colombia: Ley Estatutaria 1581 de 2012
- Chile: Ley sobre Protección de la Vida Privada
- Perú: Ley de Protección de Datos Personales
- Nicaragua: Ley de Protección de Datos Personales

- Guatemala: Ley de Protección de la Vida Privada y Datos Personales
- Costa Rica: Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales
- Jamaica: Data Privacy Act 2020
- República Dominicana: Ley sobre Protección de Datos de Carácter Personal

El Encargado auxiliará Al Responsable en asegurar el cumplimiento de estas leyes, incluidas, entre otras, las solicitudes de derechos de los sujetos de datos, evaluaciones de impacto en la protección de datos y notificaciones de violación.

## INSTRUCCIONES DE PROCESAMIENTO DE DATOS

El Encargado solo procesará datos personales siguiendo instrucciones documentadas del Responsable, incluidas las transferencias de datos personales a un tercer país o a una organización internacional, a menos que esté obligado a hacerlo por ley aplicable a la que esté sujeto el Encargado; en tal caso, el Encargado informará al Responsable sobre ese requisito legal antes de procesar, a menos que esa ley prohíba tal información por motivos importantes de interés público.

El Encargado asegurará que las personas autorizadas para procesar los datos personales se hayan comprometido a la confidencialidad o estén bajo una obligación legal adecuada de confidencialidad.

El Encargado no procesará datos personales de manera inconsistente con las instrucciones del Responsable-

## SEGURIDAD DE DATOS

El Encargado implementará medidas técnicas y organizacionales apropiadas para garantizar un nivel de seguridad adecuado al riesgo, incluyendo, entre otras:

- Pseudonimización y cifrado de datos personales.
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia continua de los sistemas y servicios de procesamiento.
- La capacidad de restaurar la disponibilidad y acceso a datos personales de forma oportuna en caso de un incidente físico o técnico.
- Un proceso para probar, evaluar y analizar regularmente la efectividad de las medidas técnicas y organizacionales para garantizar la seguridad del procesamiento.
- El Encargado notificará al Responsable sin tardanza indebida después de tener conocimiento de cualquier violación de datos personales.

## DERECHOS DE LOS SUJETOS DE DATOS

El Encargado ayudará al Responsable mediante medidas técnicas y organizacionales apropiadas en la medida de lo posible para cumplir con la obligación del Responsable de responder a las solicitudes de ejercicio de los derechos de los sujetos de datos establecidos en las leyes de protección de datos aplicables.

El Encargado notificará de inmediato al Responsable si recibe una solicitud de un sujeto de datos bajo cualquier ley de protección de datos aplicable con respecto a los datos personales procesados en nombre del Responsable. El Encargado no responderá a tal solicitud excepto siguiendo las instrucciones documentadas del Responsable o como lo exijan las leyes aplicables a las que esté sujeto el Encargado; en este caso, el Encargado informará al Responsable sobre ese requisito legal antes de responder a la solicitud, a menos que esa ley prohíba dicha información por razones importantes de interés público.

## NOTIFICACIÓN DE VIOLACIÓN DE DATOS

El Encargado notificará al Responsable sin tardanza indebida después de tener conocimiento de una violación de datos personales. Dicha notificación incluirá:

- La naturaleza de la violación de datos personales, incluyendo, cuando sea posible, las categorías y el número aproximado de sujetos de datos afectados y las categorías y el número aproximado de registros de datos personales afectados.
- Las posibles consecuencias de la violación de datos personales.
- Las medidas tomadas o que se proponen tomar por el Encargado para abordar la violación de datos personales, incluidos, cuando sea apropiado, medidas para mitigar sus posibles efectos adversos.

## EVALUACIÓN DEL IMPACTO EN LA PROTECCIÓN DE DATOS Y CONSULTA PREVIA

El Encargado ayudará al Responsable con cualquier evaluación de impacto en la protección de datos y consultas previas con autoridades de supervisión u otras autoridades competentes en materia de privacidad de datos que el Responsable considere razonablemente necesarias conforme a cualquier ley de protección de datos relevante.

Dicha asistencia incluirá, cuando sea apropiado, proporcionar al Responsable la información y documentación necesarias.

## MANTENIMIENTO DE REGISTROS

El Encargado mantendrá registros de todas las categorías de actividades de procesamiento realizadas en nombre del Responsable, que contengan:

- El nombre y los datos de contacto del Encargado y de cada Responsable en nombre del cual el Encargado está actuando y, cuando sea aplicable, del representante del Responsable o del Encargado y del oficial de protección de datos.

- Las categorías de procesamiento realizadas en nombre de cada Responsable.
- Cuando sea aplicable, transferencias de datos personales a un tercer país o a una organización internacional, incluyendo la identificación de ese tercer país o aquella organización internacional y, en el caso de transferencias referidas en leyes de protección de datos aplicables, la documentación de las salvaguardias adecuadas.
- Una descripción general de las medidas de seguridad técnicas y organizativas a las que se refiere este Acuerdo.

## DERECHOS DE AUDITORÍA

El Encargado pondrá a disposición del Responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en este Acuerdo y permitirá y contribuirá a auditorías, incluyendo inspecciones realizadas por el Responsable u otro auditor mandatado por el Responsable. Esta auditoría podrá realizarse al menos dos veces al año por el Responsable o un tercero contratado para estos fines.

El Encargado informará de inmediato al Responsable si, en su opinión, una instrucción infringe las leyes de protección de datos aplicables.

## DEVOLUCIÓN O ELIMINACIÓN DE DATOS PERSONALES

Al término del contrato, el Encargado, dentro de los 30 días siguientes a la finalización de los servicios, a elección del Responsable, eliminará o devolverá todos los datos personales al Responsable y eliminará las copias existentes, a menos que la ley aplicable requiera el almacenamiento de los datos personales.

## LEGISLACIÓN APLICABLE Y JURISDICCIÓN

Este Acuerdo se regirá e interpretará de acuerdo con las leyes DEL PAÍS EN QUE SE VENDIERON LOS BIENES O SE PROPORCIONARON LOS SERVICIOS POR PARTE DEL PROVEEDOR.

Cualquier disputa que surja o esté relacionada con este Acuerdo estará sujeta a la jurisdicción exclusiva de los tribunales del respectivo país. El Encargado cooperará con el Responsable para cumplir con las obligaciones del Responsable bajo las leyes de protección de datos aplicables.

EN TESTIMONIO DE LO CUAL, las partes del presente han ejecutado este Acuerdo a partir de la Fecha de Vigencia. CON LA ACEPTACIÓN DE LA ORDEN DE SERVICIO Y/O ORDEN DE COMPRA, EL PROVEEDOR RECONOCE Y ACEPTA LOS TÉRMINOS Y CONDICIONES CONTENIDOS EN ESTE DOCUMENTO LEGAL VINCULANTE.ESTE DOCUMENTO ES UNA PARTE INTEGRAL DE CUALQUIER ORDEN DE COMPRA Y/O SERVICIO EN EL QUE CONCENTRIX Y EL PROVEEDOR SON PARTES.

b. English

**DATA PROTECTION AGREEMENT**
**SUPPLIERS**

This Data Protection Agreement ("Agreement") is made as an amendment to the existing contractual relationship between **CONCENTRIX** (Data Processor), including its affiliated companies, and ANY **SUPPLIER** THAT PROVIDES GOOD AND/OR SERVICES in which they are processing personal data, jointly referred to as the "Parties".

**WITH THE ACCEPTANCE OF THE SERVICE ORDER AND/OR PURCHARSE ORDER, THE PROVIDER ACKNOWLEDGE AND ACCEPT THE TERMS AND CONDITIONS CONTAINED IN THIS LEGAL BINDING DOCUMENT.**

Effective Date:

Effective date of the acceptance of the purchase order and/or service order/ or express acceptance of our Policies, Manuals and/or Binding Corporate Rules, or any other legal binding document between parties.

**PURPOSE**

This Agreement outlines the responsibilities and obligations of the Processor concerning the processing of personal data on behalf of the Controller, ensuring compliance with data protection legislation across Latin America. This includes, but is not limited to, the various national data protection laws and regulations in each country within the region. The Processor shall be subjected to Concentrix Privacy Policy for Latam and the Caribbean, Data Privacy Manual, and Privacy Binding Corporate Rules. The documentation can be located here:
The Processor is committed to assisting the Controller in obtaining and maintaining the necessary consent from data subjects for the processing of their personal data. This includes ensuring that data subjects are adequately informed about the purposes of the data processing, their rights under applicable data protections laws, and any other information necessary to ensure informed consent.

**DEFINITIONS**

1. Personal Data: Any information relating to an identified or identifiable natural person.
2. Sensitive Personal Data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

3. Public Data: Information that is lawfully made available to the public from federal, state, or local government records or other publicly accessible sources.
4. Private Data: Personal data that is not publicly available and includes information such as names, addresses, social security numbers, and other identifiers.
5. Financial Data: Personal data related to an individual's financial status, including but not limited to bank account details, credit card information, financial statements, and income information.
6. Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means.
7. Data Subject: An individual whose personal data is processed.
8. Controller: The entity which determines the purposes and means of the processing of personal data.
9. Processor: The entity which processes personal data on behalf of the controller.
10. Consent: Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.

## SCOPE AND APPLICATION

This Agreement applies to all personal data processed by the Processor on behalf of the Controller, including private data, public data, sensitive data, and financial information.

This Agreement serves as an amendment to the existing contract between the Controller and the Processor, incorporating data protection requirements as stipulated by relevant legislation across Latin America.

## COMPLIANCE WITH DATA PROTECTION LAWS

The Processor shall comply with all applicable data protection laws and regulations, including but not limited to:

1. Brazil: Lei Geral de Proteção de Dados (LGPD)
2. Argentina: Ley de Protección de los Datos Personales
3. Mexico: Ley Federal de Protección de Datos Personales en Posesión de los Particulares
4. Colombia: Ley Estatutaria 1581 de 2012
5. Chile: Ley sobre Protección de la Vida Privada
6. Peru: Ley de Protección de Datos Personales
7. Nicaragua: Ley de Protección de Datos Personales
8. Guatemala: Ley de Protección de la Vida Privada y Datos Personales

9. Costa Rica: Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales
10. Jamaica: Data Protection Act
11. República Dominicana: Ley sobre Protección de Datos de Carácter Personal

The Processor shall assist the Controller in ensuring compliance with these laws, including but not limited to data subject rights requests, data protection impact assessments, and breach notifications.

## DATA PROCESSING INSTRUCTIONS

The Processor shall process personal data only on documented instructions from the Controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by applicable law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

The Processor shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

The Processor shall not process personal data in a manner inconsistent with the Controller's instructions.

## DATA SECURITY

The Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including but not limited to:

1. Pseudonymization and encryption of personal data.
2. The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
4. A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The Processor shall notify the Controller without undue delay after becoming aware of any breach of personal data.

## DATA SUBJECT RIGHTS

The Processor shall assist the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in applicable data protection laws.

The Processor shall promptly notify the Controller if it receives a request from a data subject under any applicable data protection law in respect of personal data processed on behalf of the Controller. The Processor shall not respond to such a request except on the documented instructions of the Controller or as required by applicable laws to which the Processor is subject, in which case the Processor shall inform the Controller of that legal requirement before responding to the request, unless that law prohibits such information on important grounds of public interest.

## DATA BREACH NOTIFICATION

The Processor shall notify the Controller without undue delay after becoming aware of a personal data breach. Such notification shall include:

1. The nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.
2. The likely consequences of the personal data breach.
3. The measures taken or proposed to be taken by the Processor to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

## DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

The Processor shall aid the Controller with any data protection impact assessments and prior consultations with supervisory authorities or other competent data privacy authorities, which the Controller reasonably considers to be required of any relevant data protection law.

Such assistance shall include, where appropriate, providing the Controller with necessary information and documentation.

## RECORD KEEPING

The Processor shall maintain records of all categories of processing activities carried out on behalf of the Controller, containing:

1. The name and contact details of the Processor and of each Controller on behalf of which the Processor is acting, and, where applicable, of the Controller's or Processor's representative, and the data protection officer.
2. The categories of processing carried out on behalf of each Controller.
3. Where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in applicable data protection laws, the documentation of suitable safeguards.
4. A general description of the technical and organizational security measures referred to in this Agreement.

## AUDIT RIGHTS

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Agreement and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. This audit can be done at least twice a year by the controller, or a third party hired for these purposes.

The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes applicable data protection laws.

## RETURN OR DELETION OF PERSONAL DATA

Upon termination of the contract, the Processor shall, within the 30-days after the termination of the services, at the choice of the Controller, delete or return all the personal data to the Controller and delete existing copies unless applicable law requires storage of the personal data.

## GOVERNING LAW AND JURISDICTION

This Agreement shall be governed by and construed in accordance with the laws of THE COUNTRY IN WHICH THE GOOD WAS SOLD OR THE SERVICES WAS PROVIDED BY THE PROVIDER.

Any disputes arising out of or in connection with this Agreement shall be subject to the exclusive jurisdiction of the courts of the respective Country

The Processor shall cooperate with the Controller in meeting the Controller's obligations under applicable data protection laws.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the Effective Date.

**WITH THE ACCEPTANCE OF THE SERVICE ORDER AND/OR PURCHARSE ORDER, THE PROVIDER ACKNOWLEDGE AND ACCEPT THE TERMS AND CONDITIONS CONTAINED IN THIS LEGAL BINDING DOCUMENT.**
**THIS DOCUMENT IS AN INTEGRAL PART OF ANY PURCHARSE ORDER AND/OR SERVICES IN WHICH CONCENTRIX AND THE PROVIDER ARE PARTIES.**

(c) Portuguese

CONTRATO DE PROTEÇÃO DE DADOS
FORNECEDORES

Este Contrato de Proteção de Dados ("Contrato") é feito como uma emenda ao relacionamento contratual existente entre a CONCENTRIX (Processador de Dados), incluindo suas empresas afiliadas, e QUALQUER FORNECEDOR QUE FORNECE BEM E/OU SERVIÇOS nos quais eles estão processando dados pessoais, conjuntamente denominados "Partes".

COM A ACEITAÇÃO DA ORDEM DE SERVIÇO E/OU ORDEM DE COMPRA, O PROVEDOR RECONHECE E ACEITA OS TERMOS E CONDIÇÕES CONTIDOS NESTE DOCUMENTO LEGAL VINCULATIVO.

Data de vigência:

Data de vigência da aceitação da ordem de compra e/ou ordem de serviço/ ou aceitação expressa de nossas Políticas, Manuais e/ou Regras Corporativas Vinculativas, ou qualquer outro documento legal vinculativo entre as partes.

OBJETIVO

Este Contrato descreve as responsabilidades e obrigações do Processador em relação ao processamento de dados pessoais em nome do Controlador, garantindo a conformidade com a legislação de proteção de dados em toda a América Latina. Isso inclui, mas não se limita a, as várias leis e regulamentações nacionais de proteção de dados em cada país da região. O Processador estará sujeito à Política de Privacidade da Concentrix para a América Latina e o Caribe, ao Manual de Privacidade de Dados e às Regras Corporativas Vinculativas de Privacidade. A documentação pode ser localizada aqui:

O Processador está comprometido em auxiliar o Controlador na obtenção e manutenção do consentimento necessário dos titulares dos dados para o processamento de seus dados pessoais. Isso inclui garantir que os titulares dos dados sejam adequadamente informados sobre os propósitos do processamento de dados, seus direitos sob as leis de proteção de dados aplicáveis e quaisquer outras informações necessárias para garantir o consentimento informado.

DEFINIÇÕES

1. Dados Pessoais: Qualquer informação relacionada a uma pessoa física identificada ou identificável.
2. Dados Pessoais Sensíveis: Dados pessoais que revelem origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos com a finalidade de identificar exclusivamente uma pessoa física, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa física.

3. Dados Públicos: Informações que são legalmente disponibilizadas ao público a partir de registros do governo federal, estadual ou local ou outras fontes de acesso público.
4. Dados Privados: Dados pessoais que não estão disponíveis publicamente e incluem informações como nomes, endereços, números de previdência social e outros identificadores.
5. Dados Financeiros: Dados pessoais relacionados ao status financeiro de um indivíduo, incluindo, mas não se limitando a detalhes de conta bancária, informações de cartão de crédito, demonstrações financeiras e informações de renda.
6. Processamento: Qualquer operação ou conjunto de operações que é realizada em dados pessoais ou em conjuntos de dados pessoais, seja por meios automatizados.
7. Titular dos Dados: Um indivíduo cujos dados pessoais são processados.
8. Controlador: A entidade que determina os propósitos e meios do processamento de dados pessoais.
9. Processador: A entidade que processa dados pessoais em nome do controlador.
10. Consentimento: Qualquer indicação livremente dada, específica, informada e inequívoca dos desejos do titular dos dados, pela qual ele, por uma declaração ou por uma ação afirmativa clara, significa concordância com o processamento de dados pessoais relacionados a ele.

ÂMBITO E APLICAÇÃO

Este Contrato se aplica a todos os dados pessoais processados pelo Processador em nome do Controlador, incluindo dados privados, dados públicos, dados sensíveis e informações financeiras.

Este Contrato serve como uma emenda ao contrato existente entre o Controlador e o Processador, incorporando requisitos de proteção de dados conforme estipulado pela legislação relevante em toda a América Latina.

CUMPRIMENTO DAS LEIS DE PROTEÇÃO DE DADOS O Processador deverá cumprir todas as leis e regulamentos de proteção de dados aplicáveis, incluindo, mas não se limitando a:
1. Brasil: Lei Geral de Proteção de Dados (LGPD)
2. Argentina: Ley de Protección de los Datos Personales
3. México: Ley Federal de Protección de Datos Personales en Posesión de los Particulares
4. Colômbia: Ley Estatutaria 1581 de 2012
5. Chile: Ley sobre Pro Proteção da Vida Privada
6. Peru: Lei de Proteção de Dados Pessoais
7. Nicarágua: Lei de Proteção de Dados Pessoais
8. Guatemala: Lei de Proteção da Vida Privada e Dados Pessoais
9. Costa Rica: Lei de Proteção da Pessoa frente ao Tratamento de seus Dados Pessoais
10. Jamaica: Lei de Proteção de Dados
11. República Dominicana: Lei sobre Proteção de Dados Pessoais de Carácter Personal

O Processador auxiliará o Controlador a garantir a conformidade com essas leis, incluindo, mas não se limitando a solicitações de direitos do titular dos dados, avaliações de impacto de proteção de dados e notificações de violação.

INSTRUÇÕES DE PROCESSAMENTO DE DADOS

O Processador processará dados pessoais somente mediante instruções documentadas do Controlador, inclusive com relação a transferências de dados pessoais para um terceiro país ou uma organização internacional, a menos que seja exigido por lei aplicável.

## 15. HISTORIAL DE CAMBIOS

| Versión | Fecha | Descripción |
|---|---|---|
| 1 | 29/12/2022 | Creación de Manual de Procedimientos de protección de datos personales. |
| 2 | 24/9/2024 | Correcciones menores e inclusión de lenguaje relacionado con las BCR,IA, y la inclusión del Acuerdo General de Protección de Datos Personales para Contratistas. |

## 16. FLUJO DE APROBACIÓN

| ELABORÓ | REVISÓ | APROBÓ |
|---|---|---|
| **Nombre:** Bruno Soares<br><br>**Cargo**: Analista de privacidad de Datos Concentrix | **Nombre:** Juan Andrés Trujillo Sánchez<br><br>**Cargo**: Oficial de Protección de Datos Concentrix | **Nombre:** Natalia González Lewis<br>**Cargo**: Gerente de Cumplimiento Concentrix |

## 1. OBJETIVO

O grupo de empresas que compõem a Concentrix Américas (doravante referido conjuntamente como "Concentrix") reconhece a importância da segurança, privacidade e confidencialidade das informações pessoais que usuários, clientes, fornecedores, empregados, parceiros de negócios, candidatos e terceiros possam fornecer e/ou transferir para a Concentrix através de vários canais disponibilizados, como, mas não limitado a: websites, aplicações, redes sociais, documentos físicos e/ou digitais.

Devido ao exposto, a Concentrix compromete-se a (i) proteger eficazmente os direitos dos Titulares dos Dados; e (ii) processar adequadamente os Dados Pessoais conforme a regulamentação aplicável sobre privacidade e proteção de dados pessoais.

Assim, o propósito deste Manual Interno de Privacidade e Proteção de Dados Pessoais (doravante, "Manual") é complementar as disposições gerais da Política de Tratamento de Dados Pessoais para a Concentrix Américas [https://Concentrix.com/es/news/privacy-policy-Américas/] e definir as diretrizes internas gerais aplicáveis à Concentrix para assegurar a implementação, monitoramento, manutenção e melhoria contínua dos procedimentos associados ao tratamento de dados pessoais no desenvolvimento de suas atividades.

## 2. ESCOPO

Este Manual tem como objetivo estabelecer: i) o procedimento para o tratamento de petições, reclamações e queixas relacionadas ao tratamento de dados pessoais, que será realizado internamente quando a Concentrix atuar como Responsablea de dados pessoais; e ii) o procedimento para a recepção e escalonamento para nossos clientes de petições, reclamações e queixas relacionadas ao tratamento de dados pessoais quando a Concentrix atuar como processadora de dados pessoais (doravante "Escalonamento").

Este Manual aplica-se de forma vinculativa e transversal à Concentrix Latam e o Caribe, entendida como todas as suas afiliadas e subsidiárias da Concentrix estabelecidas nas Américas, que são descritas no parágrafo 5 da Política de Tratamento de Dados Pessoais https://www.concentrix.com/legal/

Portanto, seu conhecimento e aplicação correta são obrigatórios para todos os colaboradores que fazem parte da Concentrix LATAM e o Caribe.

## 3. DEFINIÇÕES

Este Manual é regido pelas seguintes definições:

3.1. **Administrador de Banco de Dados**: É a pessoa natural vinculada à Concentrix que tem como parte de suas funções, sob um contrato de trabalho ou de serviço, o

desenvolvimento de tarefas e responsabilidades inerentes aos Bancos de Dados Pessoais da Organização. O Administrador do Banco de Dados é responsável por monitorar a devida aplicação das Políticas de Privacidade aplicáveis a cada processo e por fornecer ao oficial de proteção de dados pessoais e/ou à área de Compliance as informações necessárias para cumprir com todos os requisitos legais sobre a matéria, como o registro periódico de bancos de dados e sua atualização.

3.2. **Arquivos de Informação ou Repositórios**: Conjunto de documentos, em formato físico ou digital, mantidos pela empresa, contendo informações pessoais reguladas por lei.

3.3. **Autorização / Consentimento**: Consentimento prévio, expresso e informado dos Titulares dos Dados.

3.4. **Autoridade de Proteção de Dados**: É a autoridade encarregada em cada país de monitorar e supervisionar que os princípios, direitos e garantias dos Titulares dos Dados sejam respeitados no Tratamento de Dados Pessoais.

3.5. **Aviso de Privacidade**: É o formato físico, eletrônico ou qualquer outro formato conhecido ou a ser conhecido, que é disponibilizado ao Titular dos Dados para informar sobre o Tratamento de seus Dados Pessoais. O Aviso de Privacidade comunica aos Titulares dos Dados quem é o Responsable dos dados, as políticas de Tratamento de Dados aplicáveis, a forma de acessá-las, os direitos do Titular dos Dados e outros detalhes do tratamento.

3.6. **Banco de Dados**: Conjunto organizado de Dados Pessoais que é objeto de Tratamento.

3.7. **Cessionário**: Pessoa que adquire os direitos de outra pessoa por sucessão ou transmissão

3.8. **Colaborador Autorizado**: Colaborador da Concentrix que está autorizado, por suas funções específicas, a acessar ou dar qualquer tipo de tratamento a um banco de dados gerenciado pela Concentrix, que pode conter dados pessoais.

3.9. **Comitê de Proteção de Dados Pessoais**: Corpo interno da Concentrix integrado pelo gerente jurídico, o gerente de Compliance, os delegados da área de IT Compliance, os delegados da área de Segurança da Informação e o Encarregado de Proteção de Dados Pessoais para garantir a implementação eficaz das políticas e procedimentos adotados em conformidade com o regime geral de proteção de dados pessoais e para executar planos de ação em caso de possíveis incidentes de segurança da informação que possam afetar a integridade, confidencialidade e/ou integridade dos dados pessoais.

3.10. **Consulta**: É o pedido feito pelo Titular dos Dados sobre seus Dados Pessoais contidos nos bancos de dados da Concentrix que não estão restritos de acordo com a lei, seguindo os procedimentos estabelecidos no Programa Integral de Gestão de Dados Pessoais.

3.11. **Dados Pessoais**: Qualquer informação vinculada ou que possa ser associada a uma ou mais pessoas naturais específicas ou determináveis.

3.12. **Encarregado de Proteção de Dados Pessoais e/ou Delegado e/ou Líder Local de Proteção de Dados**: É a pessoa natural que atende ao perfil estabelecido por lei e cuja função é monitorar e controlar a aplicação da Política de Processamento de Dados Pessoais e outras políticas e procedimentos relacionados.

**Nota**: Nas regulamentações aplicáveis no Brasil, a definição acima corresponde ao termo: Encarregado de Proteção de Dados.

3.13. **Dados Sensíveis**: Dados pessoais que afetam a privacidade dos Titulares dos Dados ou cujo uso indevido pode gerar discriminação, como os dados que revelam origem racial ou étnica, orientação política, convicções religiosas ou filosóficas, filiação sindical, organizações sociais ou de direitos humanos, ou que promovem os interesses de qualquer partido político ou que garantem os direitos e garantias de partidos políticos de oposição, bem como dados relacionados à saúde, vida sexual e dados biométricos.

3.14. **Encarregado de Proteção de Dados Pessoais e/ou Delegado e/ou Líder Local de Proteção de Dados**: É a pessoa natural que atende ao perfil estabelecido por lei e cuja função é monitorar e controlar a implementação da Política de Processamento de Dados Pessoais e outras Políticas e Procedimentos, bem como a conformidade com as leis de privacidade aplicáveis.

**Nota**: Nas regulamentações aplicáveis no Brasil, a definição acima corresponde ao termo: Encarregado de Proteção de Dados.

3.15. **Escalonamento**: Procedimento para encaminhar os requisitos dos Titulares dos Dados para os clientes da Concentrix (Responsablees de Dados), para que os clientes respondam diretamente a eles.

3.16. **Processador**: Pessoa natural ou jurídica, pública ou privada, que por si só ou em associação com outros, realiza o Processamento de Dados Pessoais em nome do Responsable.

**Nota**: Nas regulamentações aplicáveis no Brasil, a definição acima corresponde ao termo: Operador.

3.17. **Habeas Data (quando aplicável)**: O direito de toda pessoa de conhecer, atualizar e retificar as informações que foram coletadas sobre ela em arquivos e bancos de dados de natureza pública ou privada.

3.18. **Incidente de Segurança ou Evento**: perda, acesso, uso não autorizado e/ou roubo de Dados Pessoais, violação dos procedimentos contidos neste Manual e nas Políticas de Privacidade e Segurança da Informação da Concentrix, entrega não autorizada de informações e Dados Pessoais a terceiros, Processamento não autorizado de Dados Pessoais sob as Políticas de Privacidade da Concentrix.

3.19. **Regras Corporativas Vinculantes**: Este é um dos mecanismos legais estabelecidos por lei que permite transferências de informações dentro de um grupo corporativo.

3.20. **PCCs**: Termo que inclui Petições, Queixas, Reclamações e Sugestões dos Titulares dos Dados das informações ou que pretendem reivindicar direitos relacionados a dados pessoais.

3.21. **Reclamação**: É o pedido feito pelos Titulares dos Dados sobre seus Dados Pessoais contidos nos bancos de dados da Concentrix, através do qual podem solicitar a exclusão de seus dados e/ou revogar a autorização concedida para o seu processamento.

3.22. **Responsable de Dados/Responsable do Tratamento**: Pessoa natural ou jurídica, pública ou privada, que por si mesma ou em associação com outras, decide sobre o banco de dados e/ou o Processamento dos dados.

**Nota**: Nas regulamentações aplicáveis no Brasil, a definição acima corresponde ao termo: Responsable.

3.23. **Subprocessador**: empresa contratada pelo processador para o processamento de dados pessoais.

3.24. **Titular dos Dados**: Pessoa natural cujos Dados Pessoais são objeto de Processamento. Eles podem ser Clientes, Fornecedores, Subcontratados, Visitantes, Colaboradores, funcionários da Concentrix, que forneceram as informações ou Dados Pessoais sob o serviço prestado pela Concentrix.

3.25. **Transferência de Dados Pessoais ou Bancos de Dados Pessoais**: É a entrega de Dados Pessoais ou Bancos de Dados Pessoais por um Responsable de Dados Pessoais a outra pessoa natural ou jurídica para que esta última atue em seu nome como Responsable dos Dados Pessoais ou Bancos de Dados recebidos.

3.26. **Transmissão de Dados Pessoais**: É a entrega de Dados Pessoais ou Bases de Dados Pessoais por um Responsable de Dados a outra pessoa natural ou jurídica para que esta, em sua capacidade como Processador de Dados, realize o

Processamento de Dados Pessoais em nome do Responsable, seguindo as obrigações delineadas no contrato firmado para tal finalidade.

3.27. **Processamento**: Qualquer operação ou conjunto de operações em Dados Pessoais, como coleta, armazenamento, uso, circulação ou exclusão.

3.28. **Incidente de Segurança de Dados Pessoais**: Qualquer violação de segurança resultando na destruição, perda ou alteração acidental ou ilegal de Dados Pessoais armazenados ou processados, ou comunicação ou acesso não autorizado a tais dados.

# 4. CONSIDERAÇÕES PRELIMINARES

## 4.1 Coleta de dados pessoais e o consentimento do Titular dos Dados

O Colaborador Autorizado para a coleta de dados pessoais deve obter e manter registro em um meio seguro da autorização para o tratamento de dados pessoais do Titular dos Dados, a menos que a lei aplicável ao tratamento de dados pessoais estipule que isso não é necessário.

Antes de qualquer tipo de Tratamento de Dados Pessoais (coleta, uso, armazenamento, circulação, transmissão, transferência, atualização, modificação, exclusão, entre outros), o Colaborador Autorizado deve verificar se os dados pessoais a serem fornecidos são estritamente necessários para cumprir os propósitos para os quais são solicitados, que estão estabelecidos na Política de Privacidade da Concentrix.

O Colaborador Autorizado não deve processar Dados Pessoais isoladamente em documentos ou manuscritos que não façam parte do respectivo Banco de Dados, o que deve ser reportado à área de Compliance e ao encarregado de proteção de dados pessoais.

Quando a coleta de informações é realizada por meios não presenciais, como página da web, aplicativo móvel e/ou Call Center, a evidência da autorização para a Coleta e Tratamento de Dados Pessoais pelo Titular dos Dados será registrada no sistema usado pelo meio não presencial (Exemplo: na página da web e no aplicativo móvel, a evidência é gerada ao clicar na caixa "Aceitar" dos checkboxes ao aceitar as Políticas de Privacidade; da mesma forma, no Call Center, a prova da autorização pode ser mantida na gravação da chamada).

Se não for possível disponibilizar ao Titular dos Dados as informações sobre as Políticas de Privacidade e os propósitos do tratamento, Avisos de Privacidade devem ser postados em locais visíveis e facilmente acessíveis, fisicamente ou digitalmente, nos locais físicos ou websites onde a coleta de dados pessoais ocorre.

## 4.2 Criação e/ou modificação de Bancos de Dados

A Concentrix possui bancos de dados previamente identificados pela área de governança de dados, cujo controle está nas mãos dos administradores de Bancos de Dados Pessoais dentro da Organização; este processo deve ter suporte e orientação da área de Compliance e do Encarregado de Proteção de Dados Pessoais.

Sempre que for realizada a criação de um novo banco de dados, assim como a modificação de Bancos de Dados Pessoais existentes, deve-se obter a aprovação da área de governança de dados e da área e/ou delegado dentro da organização para a Proteção de Dados Pessoais, através do requerimento de autorização enviado para [proteccion.dedatos@concentrix.com], para manter a rastreabilidade dos repositórios de informações e bancos de dados e fazer o respectivo relatório às autoridades de proteção de dados pessoais, quando aplicável.

## 4.3 Armazenamento adequado de dados pessoais

- Independentemente do meio de coleta de dados pessoais, seja físico ou digital, o respectivo consentimento do Titular dos Dados deve ser solicitado e mantido sob condições de segurança apropriadas e pelos parâmetros estabelecidos na Política de Tratamento de Dados Pessoais da Concentrix.

- Os Dados Pessoais devem ser armazenados em Bancos de Dados ou repositórios de informações que cumpram com as medidas de segurança definidas na Política de Segurança da Informação disponível para consulta na plataforma de gestão de documentos Isolución como SI-T-R-S-006 SEGURANÇA DA INFORMAÇÃO.

- Os bancos de dados físicos devem cumprir com medidas de segurança adequadas para prevenir a consulta, alteração e/ou perda não autorizadas de informações pessoais.

- As diretrizes e procedimentos de gestão de documentos da Concentrix devem ser cumpridos para o tratamento de qualquer documento contendo dados pessoais.

## 4.4 Circulação de Dados Pessoais

- Empregados e/ou terceiros relacionados podem compartilhar Dados Pessoais com outros Empregados, terceiros relacionados e/ou áreas da Organização quando isso for necessário para o desempenho de suas funções, dependendo das responsabilidades de seu cargo. No entanto, esse Tratamento de informações pessoais deve ser conduzido em estrita conformidade com os propósitos do tratamento das informações coletadas e de acordo com as disposições das Políticas de Privacidade da Concentrix.

- É proibido e considerado uma infração grave para Empregados e/ou terceiros circular, transferir, transmitir, enviar, compartilhar e/ou comunicar informações

pessoais do Titular dos Dados a empregados que não estão autorizados a acessá-las ou a terceiros fora da Concentrix. Se um empregado souber de um possível vazamento de informações, ele/ela deve entrar em contato com a linha de ética e informar a área de Compliance e o encarregado de proteção de dados pessoais.

- Quando um empregado receber um requerimento envolvendo o fornecimento de dados pessoais, seja de uma Autoridade ou de um indivíduo, o requerimento deve ser canalizado para a área de Compliance e/ou o Encarregado de Proteção de Dados Pessoais para avaliação e fornecimento de uma resposta, conforme o procedimento descrito nos itens 4 a 6 deste Manual.

- Em caso de dúvida ou consulta sobre o uso e circulação de Dados Pessoais em relação ao propósito pelo qual foram coletados ou sobre o tratamento de dados pessoais em geral, os empregados podem contatar a área de Compliance ou o encarregado de proteção de dados pessoais

## 4.5 Transferência e Transmissão de Dados Pessoais Coletados

A Concentrix pode transferir (de Responsable para Responsable ou de Responsable para Processador) os Dados Pessoais contidos nos bancos de dados da Organização, desde que o Titular dos Dados seja informado sobre tal propósito e que as salvaguardas estabelecidas na lei aplicável para a Transferência e/ou Transmissão de Dados Pessoais sejam cumpridas. Se a Transferência for feita para terceiros localizados em países diferentes, um acordo para a transferência internacional de dados pessoais deve ser subscrito com esse Processador, ou qualquer outra salvaguarda legal aplicável será aplicada para garantir que o processador ou sub-processador cumpra com as leis de privacidade aplicáveis e medidas de segurança e outras condições necessárias para a integridade, confidencialidade e segurança dos dados pessoais transferidos.

## 4.6 Processamento de Dados Pessoais de Crianças e Adolescentes

O tratamento dos Dados Pessoais de crianças e adolescentes deve ser realizado excepcionalmente, considerando os propósitos do tratamento de dados, o respeito aos seus direitos fundamentais e o seu melhor interesse. Da mesma forma, será necessária a autorização da pessoa com autoridade parental ou representante legal.

O Colaborador e/ou terceiro que, devido às suas funções, processará os Dados Pessoais de crianças e adolescentes, deve implementar medidas especiais de confidencialidade e segurança.

O site da Concentrix não é destinado a crianças menores de treze (13) anos, e recomenda-se que ninguém com menos de treze (13) anos o utilize.

## 4.7 Processamento de dados sensíveis

Para cumprir com propósitos legais e previamente estabelecidos, podemos coletar dados considerados sensíveis, como dados relacionados à saúde, origem racial ou étnica, orientação política, convicções religiosas ou filosóficas, filiação a sindicatos, organizações sociais, direitos humanos, preferências pessoais e/ou interesses, dados biométricos, assinaturas, impressões digitais e outros dados biométricos, assim como imagens, fotografias, vídeos, vozes e/ou sons, dados de vídeo e áudio que identificam ou tornam nossos usuários, clientes, fornecedores, empregados e candidatos e/ou qualquer outra pessoa que seja ou transite em qualquer local onde a Concentrix instalou equipamentos e informações, bem como dispositivos para o controle de movimento e vigilância em geral ou preferências pessoais.

Os Titulares dos Dados não serão obrigados, em nenhuma circunstância, a autorizar o tratamento de dados sensíveis ou de menores. Não obstante, nos casos em que, para possibilitar a prestação do serviço, os Titulares dos Dados fornecerem quaisquer dados pessoais sensíveis, eles devem consentir expressamente à Concentrix o tratamento da informação ou dados pessoais sensíveis.

Portanto, o Tratamento de Dados Sensíveis só poderá ser realizado quando a lei aplicável permitir e com a autorização expressa do Titular dos Dados, exceto pelas exceções previstas em lei. Além disso, os Dados Pessoais Sensíveis coletados serão armazenados em bancos de dados e/ou arquivos especialmente protegidos e com acesso restrito apenas aos empregados que, devido às suas funções específicas, devem ter acesso a eles para garantir sua proteção aprimorada.

O colaborador e/ou terceiro encarregado que, devido às suas funções, é obrigado a tratar dados sensíveis deve ser especialmente diligente para salvaguardar sua integridade, confidencialidade e segurança. Portanto, o Tratamento de Dados Sensíveis só pode ser realizado quando a lei aplicável permitir e com a autorização expressa do Titular dos Dados, exceto pelas exceções previstas em lei.

## 5. BOAS PRÁTICAS AO RESPONDER A REQUISITOS E PCCs

Para processar qualquer requisito ou PCC, os seguintes passos devem ser seguidos:

5.1. Identificar o objeto do Requisito para fornecer uma resposta direta, clara e concreta; ao gerar novos Bancos de Dados contendo Dados Pessoais, a área responsável deve garantir a conformidade com as disposições das Políticas e Procedimentos de segurança da informação e gestão de documentos da Concentrix.

5.2. Mencionar os fatos que permitem uma compreensão lógica das respostas.

5.3. Fazer referência precisa a documentos que são enviados ou entregues como anexos, para que haja uma conexão causal entre o Requisito e as respostas.

5.4. Declarar concretamente as justificativas legais, técnicas e/ou contratuais que são aplicáveis ou necessárias.

5.5. Quando houver situações que possam ser melhoradas e/ou corrigidas, reportar as medidas que estão sendo estudadas ou que serão adotadas.

5.6. Garantir que a resposta não cause retrabalho ou repetição por parte da Autoridade Competente ou do Titular dos Dados.

5.7. Listar no final de cada resposta os respectivos anexos ou arquivos, indicando brevemente sua finalidade e declarando seu conteúdo ou nome, devidamente numerados.

5.8. Abster-se de enviar informações e documentos que não são solicitados ou que não estão relacionados ao Requisito.

5.9. Documentar a resposta a todos os Requisitos (verbais, físicos ou eletrônicos) por meio do respectivo arquivo.

5.10. Manter em local seguro uma cópia da resposta aos requisitos e seus respectivos anexos.

5.11. Quando os requisitos do Titular dos Dados ou das Autoridades Competentes forem pouco claros ou contiverem imprecisões formais que possam afetar a resposta, contatar a Autoridade Competente com antecedência suficiente antes do prazo devido para esclarecer os pontos em questão, sem exceder o limite máximo de tempo legal para responder ao requisito.

# 6. PROCEDIMENTO PARA TRATAMENTO DE REQUISITOS DE AUTORIDADES COMPETENTES

Empregados encarregados de receber, responder e enviar requisitos devem seguir o seguinte procedimento para responder a requisitos de autoridades competentes, independentemente do tipo de requisito:

## 6.1. Recebimento do requisito da autoridade competente

Se um empregado da Concentrix receber um Requisito relacionado a dados pessoais ou qualquer tipo de dado pessoal por qualquer canal de recepção, isso, em um período não superior a um (1) dia útil, deve comunicar e notificar, conforme apropriado, ao e-mail: proteccion.dedatos@concentrix.com, ao encarregado de proteção de dados pessoais / área de Compliance e ao seu superior imediato.

A não conformidade com este dever pode ser considerada má conduta grave.

## 6.2 Envio do requisito para a área responsável

Uma vez recebido o Requisito, a área ou unidade designada pela Concentrix para recebê-lo deve estabelecer e identificar o tipo de requisito e seu propósito para direcioná-lo à área responsável por respondê-lo.

Para determinar a área ou departamento da Concentrix que deve responder ao Requisito, os seguintes critérios devem ser considerados:

| Tipo de requisito | Área ou Departamento Responsável por Responder ao Requisito | Informações de Contato |
|---|---|---|
| Requisitos relacionados à prevenção, investigação e punição de atos de corrupção. | Departamento de Compliance | E-mail: natalia.lewis@Concentrix.com |
| Requisitos relacionados a riscos trabalhistas e de saúde ocupacional: | Departamento de Recursos Humanos | E-mail: relaciones.laborales.co@onelinkbpo.com |
| Requisitos relacionados ao tratamento de dados pessoais: | Departamento de Privacidade / Dados Pessoais | E-mail: protección.dedatos@concentrix.com |
| Requisitos relacionados a concorrência desleal, práticas restritivas e propriedade intelectual. Questões de e-commerce e proteção ao consumidor | Departmento Jurídico | E-mail: juliancamilo.diaz@Concentrix.com |
| Requisitos relacionados à Gestão de Pensões e Parafiscais: | Departamento de Recursos Humanos | E-mail: relaciones.laborales.co@onelinkbpo.com |

## 6.3 Determinação da competência da Concentrix

Se a Concentrix não for competente para responder ao Requisito, deve informar imediatamente a Autoridade Competente, se atuar verbalmente, ou dentro de dois (2) dias úteis após o recebimento, se o Requisito for recebido por escrito ou eletronicamente.

## 6.4 Determinar se o aplicativo está completo ou se informações ou suporte adicionais devem ser solicitados.

No caso de o requisito ser pouco claro ou incompleto, será solicitado esclarecimento à autoridade solicitante o mais breve possível e dentro de um máximo de dois (2) dias úteis após a data de recebimento; uma vez recebida a informação necessária, uma resposta imediata será dada ao requisito para cumprir dentro do prazo estabelecido pela autoridade competente.

## 6.5 Estabelecer se o Requisito envolve dados pessoais ou informações confidenciais ou proprietárias da Concentrix.

Quando o Requisito envolver a divulgação ou fornecimento de informações confidenciais ou proprietárias, a Concentrix deve informar a Autoridade Competente na resposta ao Requisito.

Da mesma forma, no caso dos Titulares dos Dados cujos dados pessoais são processados pela Concentrix, uma vez que o requisito tenha sido preparado pela área encarregada de fornecer as informações, ele deve ser revisado pela área de Compliance e pelo encarregado de proteção de dados pessoais da Concentrix para aprovar a resposta e verificar se ela cumpre os requisitos das regulamentações sobre o tratamento de dados pessoais.

Os Titulares dos Dados são aquelas pessoas naturais ou jurídicas que são contratantes, clientes, fornecedores ou parceiros comerciais da Concentrix, cujas informações confidenciais ou reservadas podem ser requeridas em um Requisito.

## 6.6 Preparação da resposta ao requisito

A resposta ao requisito será feita pela área da Concentrix encarregada de fornecer as informações requeridas. A resposta deve cumprir com os seguintes requisitos: i) oportuna; ii) objetiva; iii) verdadeira; iv) completa; v) fundamentada; e vi) atualizada.

- É oportuna quando é apresentada dentro dos prazos estipulados por lei (ou no requisito, se for feito por uma autoridade pública).

- É objetiva quando é respondida com base no conteúdo dos documentos e das evidências anexadas.

- É verdadeira quando seu conteúdo é verificável de acordo com os documentos e evidências anexados.

- É completa quando cada uma das perguntas e/ou requisitos do Requisito são respondidos.

- É fundamentada quando há justificativa para as diferentes disposições incluídas na resposta ao Requisito.

- É atualizada quando se baseia em informações e dados atualizados.

- Nos casos em que os Requisitos têm diferentes requisitos ou perguntas, estes devem ser respondidos na mesma ordem em que são solicitados e de maneira clara.

## 6.7 Procedimento para submeter uma resposta

- Independentemente do meio pelo qual o Requisito foi recebido, a resposta será enviada por escrito, seja eletronicamente (como e-mail) ou fisicamente, conforme indicado pela Autoridade Competente.

- A resposta ao requisito deve ser enviada ao endereço físico ou eletrônico indicado no requisito ou aos meios oficiais da autoridade que fez o requisito.

- A resposta ao Requisito deve ser dirigida à Autoridade Competente e ao oficial que fez o requisito.

- Para comprovar o envio, o recebimento e o número do Requisito devem ser mantidos.

## 6.8 Prazo para responder ao requisito da autoridade competente

A menos que seja estipulado de outra forma por lei ou disposição especial, os Requisitos devem ser resolvidos dentro do prazo delineado no requisito. Quando, em casos excepcionais, não for possível resolver o Requisito dentro do período mencionado, a Concentrix, por meio da área competente encarregada de responder e/ou à qual o Requisito foi endereçado, deve informar a Autoridade Competente sobre tal circunstância, declarando os motivos do atraso e indicando o prazo razoável dentro do qual o Requisito será resolvido ou uma resposta será fornecida.

# 7. PROCEDIMENTO PARA RESPONDER A PCCs RELACIONADOS AO TRATAMENTO DE DADOS PESSOAIS

Este procedimento se aplica apenas quando a Concentrix atua como Responsablea de dados pessoais, uma vez que, quando atua como Processadora, deve seguir o procedimento de "Escalonamento" previamente estabelecido com o cliente para transferir os PCCs aos contatos informados pelo cliente, e o cliente deve responder diretamente a eles. (esta é a regra geral quando fornecemos serviços de BPO para nossos clientes e eles nos dão acesso a informações pessoais dos usuários finais/clientes para que a Concentrix possa cumprir com o objeto do acordo com o cliente).

## 7.1. Quando a Concentrix é a responsável pelos dados pessoais

Os usuários, clientes, fornecedores, empregados ou candidatos da Concentrix têm o direito de saber os detalhes do tratamento de seus dados e exercer seus direitos como Titulares dos Dados, usando consultas, requisitos e reclamações sob os termos da regulamentação de proteção de dados aplicável e pelas disposições desta Política de Privacidade.

Para os fins acima, este Manual define o procedimento geral para o exercício dos direitos dos Titulares dos Dados, sem prejuízo da aplicação de procedimentos e requisitos específicos que as leis locais de cada território possam contemplar. Em caso de discrepância entre o procedimento geral estabelecido neste Manual e os procedimentos ou requisitos específicos contidos nas leis locais aplicáveis de cada território, estas últimas prevalecerão.

### 7.1.1 Recepção de PCCs (correio, balcão, fax e/ou e-mail).

As aplicações podem ser apresentadas por escrito, fisicamente e/ou digitalmente, e através dos canais habilitados pela Organização para este fim, que são:

iv) Pessoalmente, seja verbalmente ou por escrito, nos espaços físicos providenciados pela Concentrix para tais fins, como os escritórios localizados em Calle 63 # 24 - 80 em Bogotá - Colômbia.

v) Por telefone, no seguinte número: (+57) 4 444 38 20

vi) Para o correio físico ou postal, conforme o país correspondente

vii) E-mails: proteccion.dedatos@concentrix.com

Se um empregado da Concentrix receber um Requisito relacionado a dados pessoais através de canais de recepção diferentes dos mencionados nesta seção, ele deve, em no máximo um (1) dia útil, comunicar e notificar, conforme apropriado, o seguinte endereço de e-mail: proteccion.dedatos@concentrix.com, o encarregado de proteção de dados pessoais/área de Compliance e seu superior imediato.

A não conformidade com este dever pode ser considerada má conduta grave.

### 7.1.2 Determinar se a Concentrix é competente

Após o recebimento do Requisito, o Departamento de Compliance ou o Encarregado de Proteção de Dados Pessoais determinará se a Concentrix é competente para resolver o requisito.

Se a Concentrix não for competente, ela informará o Titular dos Dados ou a parte interessada dentro de dois (2) dias úteis após o recebimento (a menos que acordado de outra forma no contrato ou outro documento assinado com o cliente).

### 7.1.3 Determinar se o requerente tem legitimidade para fazer a aplicação

É essencial determinar se o requerente tem legitimidade para fazer o requerimento; isso dependerá da lei aplicável, mas, como regra geral, o requerente deve ser: i) o Titular dos Dados; ii) seu representante legal; iii) uma pessoa devidamente autorizada pelo Titular dos Dados para fazer a consulta ou reclamação; ou iv) seu herdeiro legal, pois a entrega de informações pessoais, a modificação ou a exclusão delas, quando não for a pessoa autorizada por lei a fazê-lo, pode resultar em uma violação da proteção de dados pessoais e afetar negativamente a Concentrix. Portanto, deve-se considerar o seguinte:

- Titular dos Dados e/ou quem exerce o direito em seu nome deve comprovar sua identidade para evitar perda, consulta, uso ou acesso não autorizado ou fraudulento por uma pessoa diferente do Titular dos Dados e/ou quem não tem um mandato legal para agir em seu nome.

- A acreditação pelo Titular dos Dados ou pela pessoa autorizada será feita enviando uma cópia física ou digital do documento de identificação relevante, de acordo com o meio de apresentação da consulta.

- Quando o requerimento for feito por uma pessoa diferente do Titular dos Dados, o terceiro deve comprovar devidamente a capacidade legal ou mandato para agir em nome do Titular dos Dados, enviando os documentos comprobatórios.

O requerimento será supervisionado pela área e/ou delegado encarregado dentro da organização para a proteção de dados pessoais apenas quando a identidade puder ser acreditada e os requisitos mencionados acima forem atendidos.

### 7.1.4 Determinar se o aplicativo está completo ou se informações ou suporte adicionais devem ser solicitados.

O requerimento para o exercício de qualquer um dos direitos deve conter, no mínimo, as seguintes informações:

- Nome do Interessado, seu representante e/ou a pessoa que exerce o direito em seu nome e número de identificação.

- Requerimento concreto, preciso e justificado para consulta e o direito invocado.

- Endereço físico e/ou eletrônico para notificações.

- Documentos de suporte (se aplicável).

- Assinatura do requerente, de acordo com o meio do requerimento.

Se o requerimento estiver incompleto, o interessado será solicitado, dentro de cinco (5) dias úteis a partir da data de recebimento, a corrigir as deficiências.

A informação solicitada deve ser submetida pelo requerente dentro de dois (2) meses após o requerimento; caso contrário, será entendido como uma renúncia.

Uma vez que a identidade possa ser acreditada e os requisitos mencionados acima sejam atendidos, o requerimento será tratado pela área e/ou delegado encarregado para a proteção de dados pessoais, com o apoio das outras áreas que devem fornecer informações relevantes para fornecer a resposta correspondente.

### 7.1.5 Redirecionamento do requerimento

Se for determinado que a Concentrix é competente para responder, procederá para determinar se o requerimento é de natureza técnica ou legal, ou tem uma parte técnica e uma parte legal, para direcioná-lo à área responsável pela resposta.

Se o requerimento for inteiramente de natureza legal, a área de Compliance ou o Encarregado de Proteção de Dados Pessoais procederá para resolvê-lo diretamente; caso contrário, o suporte será solicitado da área de Segurança da Informação e/ou da área responsável por responder ao requerimento.

### 7.1.6 Elaboração da resposta ao requerimento

A resposta ao requerimento deve ser oportuna, objetiva, verdadeira, completa, fundamentada e atualizada.

- É oportuna quando é apresentada dentro dos prazos estipulados por lei ou no requerimento.
- É objetiva quando é respondida com base no conteúdo dos documentos e das evidências anexadas.
- É verdadeira quando seu conteúdo é verificável de acordo com os documentos e evidências anexados.
- É completa quando cada uma das perguntas e/ou requisitos específicos do requerimento são respondidos.
- É fundamentada quando há justificativa para as diferentes disposições incluídas na resposta ao requerimento.
- É atualizada quando se baseia em informações e dados atualizados.

- Nos casos em que os Requisitos têm diferentes requisitos ou perguntas, estes devem ser respondidos claramente e na mesma ordem em que são solicitados.

### 7.1.7 Procedimento para submeter uma resposta

- Independentemente do meio pelo qual o Requisito foi recebido, a resposta será enviada por escrito, seja eletronicamente (como e-mail) ou fisicamente, conforme indicado pela Autoridade Competente.

- A resposta ao Requisito será enviada ao endereço físico ou eletrônico indicado pelo Titular dos Dados ou pelo requerente interessado.

- A resposta ao Requisito será dirigida ao requerente que fez o requerimento.

- Para comprovar o envio, o recebimento e o número do requerimento devem ser mantidos.

### 7.1.8 Prazo para responder a PCCs

O prazo máximo que a Concentrix Américas tem para responder ao requerimento é de quinze (15) dias úteis a partir do dia seguinte à data de recebimento. Quando não for possível responder ao requerimento dentro deste prazo, a parte interessada será informada sobre os motivos do atraso e a data em que o requerimento será respondido, o que não pode exceder oito (8) dias úteis após o término do primeiro prazo.

## 7.2 Quando a Concentrix supervisiona dados pessoais (Escalonamento)

Quando a Concentrix recebe PCCs de Titulares dos Dados a respeito de seus dados pessoais e atua apenas como processadora de dados, ela encaminha os requisitos recebidos para o Responsable de dados (cliente) através do procedimento de Escalonamento que foi previamente estabelecido, para que o cliente dê uma resposta direta aos requerentes/Titulares dos Dados.

O procedimento de Escalonamento e os detalhes de contato para escalar os requisitos dos Titulares dos Dados devem ser previamente estabelecidos pelo cliente e descritos nos acordos que a Concentrix subscreve com o cliente no momento de iniciar sua relação contratual.

- Prepare um roteiro de escalonamento para o tratamento de dados pessoais que inclui as diretrizes gerais sobre como abordar um PCC nos canais disponíveis para o Responsable para o tratamento de dados pessoais.

- Aprovação do Responsable de dados pessoais no roteiro de escalonamento.

- Socializar o roteiro de escalonamento com áreas operacionais e de treinamento para sua implementação.

# 8. MEDIDAS DE SEGURANÇA E INCIDENTES DE SEGURANÇA

## 8.1 Medidas de Segurança

A Concentrix definiu e implementou as medidas de segurança relevantes para a proteção das informações pessoais de todos os nossos clientes, colaboradores, fornecedores e acionistas, que foram estabelecidas com base em padrões e regulamentações internacionais, como ISO27001:2013, PCI-DSS (Padrão de Segurança de Informações de Cartão de Crédito) e SOX (Lei Sarbanes-Oxley).

As medidas de segurança são estabelecidas na Política de Segurança da Informação, bem como nas Políticas Específicas e Procedimentos e Padrões de Segurança mencionados abaixo:

- Política de Segurança da Informação
- Política de Gerenciamento de Incidentes
- Política de Criptografia
- Política de Gerenciamento de Ativos de Informação
- Política de Gerenciamento de Acesso Política de Segurança Operacional

## 8.2 Eventos de não conformidade com a Política de Privacidade, Política de Segurança da Informação e regulamentações aplicáveis.

No caso de um possível Incidente de Segurança em relação ao Tratamento de Dados Pessoais, isso deve ser relatado à área e/ou delegado dentro da Organização para a Proteção de Dados Pessoais, para qualquer um dos seguintes e-mails: proteccion.dedatos@concentrix.com, pelo colaborador ou colaboradores que tiveram conhecimento disso imediatamente após sua ocorrência, para iniciar a investigação relevante, o plano de ação e as medidas corretivas, e o respectivo relatório é feito às áreas internas e autoridades competentes dentro dos prazos estabelecidos pela Lei, se aplicável.

# 9. RESPONSABILIDADE PELO TRATAMENTO DOS BANCOS DE DADOS DA CONCENTRIX

Cada uma das áreas e colaboradores que gerenciam dados pessoais no desempenho de suas funções é responsável pela gestão adequada de bancos de dados e outros repositórios de informações contendo dados pessoais, e por cumprir com as políticas e procedimentos da Concentrix relacionados ao tratamento de dados pessoais, segurança da informação e gestão de documentos. Da mesma forma, eles devem fornecer de maneira oportuna e completa as informações necessárias pela área de Compliance e/ou o encarregado de proteção de dados pessoais e colaborar com essas áreas para facilitar o cumprimento dos requisitos legais sobre a matéria.

# 10. PENALIDADES POR NÃO CONFORMIDADE NO TRATAMENTO DE DADOS PESSOAIS

## 10.1 Sanções da Concentrix

As sanções que as autoridades competentes podem impor aos Colaboradores e à Concentrix variam de acordo com as regulamentações aplicáveis de acordo com o país ou países em que as Obrigações de Proteção de Dados Pessoais sejam violadas, que podem consistir em, mas não estão limitadas a:

- Multas de natureza Pessoal e Institucional que podem ser sucessivas enquanto a não conformidade que as originou subsistir. Suspensão das atividades relacionadas ao Tratamento de Dados Pessoais.

- O ato de suspensão indicará as medidas corretivas a serem adotadas.

- Encerramento temporário das operações relacionadas ao Tratamento de Dados Pessoais, uma vez transcorrido o prazo de suspensão sem que as medidas corretivas ordenadas pela autoridade competente tenham sido adotadas.

- Encerramento imediato e definitivo da operação que envolve o Tratamento de Dados Sensíveis.

## 10.2 Sanções aos Empregados

No caso de não conformidade com as políticas e procedimentos de Proteção de Dados Pessoais estabelecidos neste Manual, a Concentrix contempla sanções administrativas para todos os empregados, que, de acordo com sua responsabilidade no evento e a gravidade da não conformidade, podem levar à rescisão do relacionamento contratual. Da mesma forma, o Comitê de Ética, para garantir a conformidade com o Código de Ética da Concentrix e Padrões de Conduta, tem a função de conhecer, analisar, avaliar, processar, determinar e notificar infrações, reclamações e alegações relacionadas à proteção de dados pessoais.

Empregados que têm acesso a informações pessoais em razão de suas funções na Concentrix são obrigados a não divulgar, comentar, copiar, entregar, comunicar, dar acesso, trocar ou comercializar de qualquer forma ou por qualquer meio seu usuário e/ou senha e/ou outras credenciais de acesso aos sistemas e plataformas, sejam da Concentrix, do cliente ou de terceiros, que foram disponibilizados a eles, bem como qualquer informação pessoal de clientes, consumidores finais, colegas de trabalho e quaisquer outros dados pessoais recebidos ou conhecidos por eles por ocasião ou para o desempenho de suas funções. Da mesma forma, eles têm o dever de adotar medidas de segurança adequadas e relatar imediatamente qualquer roubo, alteração ou perda de suas credenciais, informações confidenciais ou dados pessoais, imediatamente ao tomar conhecimento disso. O não cumprimento desta obrigação legal e contratual resultará em penalidades disciplinares, civis e/ou criminais, conforme apropriado.

## 11. USO DE INTELIGÊNCIA ARTIFICIAL E DADOS PESSOAIS

A Concentrix, comprometida com a evolução tecnológica para melhorar os serviços de nossos clientes e a experiência de nossos funcionários, acionistas, usuários e, em geral, qualquer detentor das informações, adotou o desenvolvimento e o uso de tecnologias de Inteligência Artificial sob a declaração de uso ético e princípio contra a inteligência artificial da Concentrix: https://www.concentrix.com/wp-content/uploads/2024/04/Concentrix-Generative-AI-Statement.pdf.

Portanto, a Concentrix, na implementação e no desenvolvimento da tecnologia de IA, levará em conta a declaração de princípios para a proteção de dados pessoais processados. Da mesma forma, terá como princípios orientadores: (i) Privacidade por Design e por Padrão; (ii) Princípio da Minimização de Dados Pessoais e; (iii) As obrigações impostas pelos regulamentos atuais sobre Inteligência Artificial onde temos presença comercial.

A Concentrix está comprometida com o uso responsável e ético de qualquer avanço tecnológico, especialmente em relação à proteção abrangente dos dados pessoais pelos quais somos responsáveis e encarregados.

## 12. NORMAS CORPORATIVAS VINCULANTES - REFERÊNCIA AO MANUAL DE PROTEÇÃO DE DADOS DA CONCENTRIX.

As Regras Corporativas Vinculantes (“NCR” e/ou “BCR”), relativas à proteção de dados, são obrigatórias para o grupo empresarial Concentrix quando as empresas que compõem o grupo transferem, ou conjunto de transferências, de dados pessoais para outro processador dentro de uma jurisdição onde a Concentrix opera, ou para outro país onde a empresa também opera.

Para esse fim, a Concentrix, em conformidade com os regulamentos de proteção de dados pessoais das jurisdições onde opera na América Latina e no Caribe, implementou um compêndio de Regras Corporativas Vinculantes sobre proteção de dados pessoais, que foram incluídas em nosso Manual de Regras Corporativas Vinculantes, que pode ser encontrado em: https://www.concentrix.com/legal/ na seção Políticas de Nível GEO e subseção LATAM.

Em nosso Manual, você pode encontrar todas as BCRs da Concentrix aplicáveis à transferência de dados pessoais e outros aspectos relacionados à privacidade.

## 13. ACORDO GERAL DE PROTEÇÃO DE DADOS PARA CONTRATADOS

Em virtude dos requisitos normativos em matéria de proteção de dados pessoais nas jurisdições nas quais temos presença comercial, e o interesse do Grupo Concentrix em gerar confiança para nossos titulares sobre as medidas contratuais estabelecidas para

proteger seus dados pessoais, elaboramos um Acordo Geral de Proteção de Dados para Contratantes da Concentrix, que estabelece de forma padrão as medidas contratuais, organizacionais, administrativas, humanas e técnicas que os Contratantes, que prestam serviços envolvendo o tratamento de dados de funcionários e/ou acionistas, devem cumprir para prestar serviços à Concentrix.

Dessa forma, cada Contratante, ao preencher e assinar os formulários de fornecedores, ordens de serviço, ordens de compra, carta de aceitação, carta de oferta e qualquer documento comercial vinculante entre a Concentrix e o Contratante, aceita, de forma expressa e inequívoca, o conteúdo do Acordo Geral de Proteção de Dados para Contratantes, o qual será o anexo 1 do presente Manual, tanto em espanhol quanto em inglês.

## ANEXO I – ACORDO PADRÃO DE PROTEÇÃO DE DADOS PESSOAIS PARA CONTRATADOS

### a. Español

Este Acuerdo de Protección de Datos ('Acuerdo') se realiza como una enmienda a la relación contractual existente entre CONCENTRIX (Encargado de Datos) incluyendo sus empresas afiliadas y CUALQUIER PROVEEDOR QUE PROPORCIONE BIENES Y/O SERVICIOS en los que se procesen datos personales, referidos conjuntamente como las 'Partes'.

**CON LA ACEPTACIÓN DE LA ORDEN DE SERVICIO Y/O ORDEN DE COMPRA, EL PROVEEDOR RECONOCE Y ACEPTA LOS TÉRMINOS Y CONDICIONES CONTENIDOS EN ESTE DOCUMENTO LEGAL VINCULANTE.**

Fecha de Vigencia:

Fecha de vigencia de la aceptación de la orden de compra y/o orden de servicio o aceptación expresa de nuestros Manuales de Políticas y/o Reglas Corporativas Vinculantes o cualquier otro documento legal vinculante entre las partes.

**OBJETO**

Este Acuerdo describe las responsabilidades y obligaciones del Encargado con respecto al procesamiento de datos personales en nombre del Responsable, garantizando el cumplimiento de la legislación de protección de datos en toda América Latina. Esto incluye, pero no se limita a, las diversas leyes y regulaciones nacionales de protección de datos en cada país de la región. El Encargado estará sujeto a la Política de Privacidad de Concentrix para Latam y al Manual de Privacidad de Datos y Reglas Corporativas Vinculantes para el Caribe. La documentación se puede encontrar aquí: El Encargado se compromete a ayudar al Responsable a obtener y mantener el consentimiento necesario de los sujetos de datos para el procesamiento de sus datos personales. Esto incluye garantizar que los sujetos de datos estén adecuadamente informados sobre los propósitos del procesamiento de datos,

sus derechos bajo las leyes de protección de datos aplicables y cualquier otra información necesaria para asegurar el consentimiento informado.

## DEFINTICIONES

- **Datos Personales:** Cualquier información relacionada con una persona natural identificada o identificable.

- **Datos Personales Sensibles:** Datos personales que revelan el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos con el fin de identificar de forma única a una persona natural, datos sobre salud o datos sobre la vida sexual o la orientación sexual de una persona natural.
- **Datos Públicos:** Información que se pone a disposición del público de manera legal a partir de registros gubernamentales federales, estatales o locales, o de otras fuentes accesibles al público.

- **Datos Privados:** Datos personales que no están disponibles públicamente e incluyen información como nombres, direcciones, números de seguridad social y otros identificadores.

- **Datos Financieros:** Datos personales relacionados con el estado financiero de un individuo, incluidos, entre otros, detalles de cuentas bancarias, información de tarjetas de crédito, estados financieros e información de ingresos.

- **Procesamiento:** Cualquier operación o conjunto de operaciones que se realicen sobre datos personales o sobre conjuntos de datos personales, ya sea por medios automatizados.

- **Titulares:** Un individuo cuyos datos personales son procesados.

- **Responsable:** La entidad que determina los propósitos y medios del procesamiento de datos personales.

- **Encargado:** La entidad que procesa datos personales en nombre del Responsable.

- **Consentimiento:** Cualquier indicación específica, informada y no ambigua de los deseos del sujeto de datos mediante la cual, mediante una declaración o acción afirmativa clara, manifiesta su acuerdo para el procesamiento de datos personales que los concierne.

## ALCANCE Y APLICACIÓN

Este Acuerdo se aplica a todos los datos personales procesados por el Encargado en nombre del Responsable, incluidos datos privados, datos públicos, datos sensibles e información financiera. Este Acuerdo sirve como una enmienda al contrato existente entre

el Responsable y el Encargado, incorporando los requisitos de protección de datos estipulados por la legislación relevante en toda América Latina.

## CUMPLIMIENTO DE LAS LEYES DE PROTECCIÓN DE DATOS

- Brasil: Ley General de Protección de Datos (LGPD)
- Argentina: Ley de Protección de los Datos Personales
- México: Ley Federal de Protección de Datos Personales en Posesión de los Particulares
- Colombia: Ley Estatutaria 1581 de 2012
- Chile: Ley sobre Protección de la Vida Privada
- Perú: Ley de Protección de Datos Personales
- Nicaragua: Ley de Protección de Datos Personales
- Guatemala: Ley de Protección de la Vida Privada y Datos Personales
- Costa Rica: Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales
- Jamaica: Ley de Protección de Datos
- República Dominicana: Ley sobre Protección de Datos de Carácter Personal

El Encargado auxiliará Al Responsable en asegurar el cumplimiento de estas leyes, incluidas, entre otras, las solicitudes de derechos de los sujetos de datos, evaluaciones de impacto en la protección de datos y notificaciones de violación.

## INSTRUCCIONES DE PROCESAMIENTO DE DATOS

El Encargado solo procesará datos personales siguiendo instrucciones documentadas del Responsable, incluidas las transferencias de datos personales a un tercer país o a una organización internacional, a menos que esté obligado a hacerlo por ley aplicable a la que esté sujeto el Encargado; en tal caso, el Encargado informará al Responsable sobre ese requisito legal antes de procesar, a menos que esa ley prohíba tal información por motivos importantes de interés público.

El Encargado asegurará que las personas autorizadas para procesar los datos personales se hayan comprometido a la confidencialidad o estén bajo una obligación legal adecuada de confidencialidad.

El Encargado no procesará datos personales de manera inconsistente con las instrucciones del Responsable-

## SEGURIDAD DE DATOS

El Encargado implementará medidas técnicas y organizacionales apropiadas para garantizar un nivel de seguridad adecuado al riesgo, incluyendo, entre otras:

- Pseudonimización y cifrado de datos personales.

- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia continua de los sistemas y servicios de procesamiento.
- La capacidad de restaurar la disponibilidad y acceso a datos personales de forma oportuna en caso de un incidente físico o técnico.
- Un proceso para probar, evaluar y analizar regularmente la efectividad de las medidas técnicas y organizacionales para garantizar la seguridad del procesamiento.
- El Encargado notificará al Responsable sin tardanza indebida después de tener conocimiento de cualquier violación de datos personales.

## DERECHOS DE LOS SUJETOS DE DATOS

El Encargado ayudará al Responsable mediante medidas técnicas y organizacionales apropiadas en la medida de lo posible para cumplir con la obligación del Responsable de responder a las solicitudes de ejercicio de los derechos de los sujetos de datos establecidos en las leyes de protección de datos aplicables.

El Encargado notificará de inmediato al Responsable si recibe una solicitud de un sujeto de datos bajo cualquier ley de protección de datos aplicable con respecto a los datos personales procesados en nombre del Responsable. El Encargado no responderá a tal solicitud excepto siguiendo las instrucciones documentadas del Responsable o como lo exijan las leyes aplicables a las que esté sujeto el Encargado; en este caso, el Encargado informará al Responsable sobre ese requisito legal antes de responder a la solicitud, a menos que esa ley prohíba dicha información por razones importantes de interés público.

## NOTIFICACIÓN DE VIOLACIÓN DE DATOS

El Encargado notificará al Responsable sin tardanza indebida después de tener conocimiento de una violación de datos personales. Dicha notificación incluirá:

- La naturaleza de la violación de datos personales, incluyendo, cuando sea posible, las categorías y el número aproximado de sujetos de datos afectados y las categorías y el número aproximado de registros de datos personales afectados.
- Las posibles consecuencias de la violación de datos personales.
- Las medidas tomadas o que se proponen tomar por el Encargado para abordar la violación de datos personales, incluidos, cuando sea apropiado, medidas para mitigar sus posibles efectos adversos.

## EVALUACIÓN DEL IMPACTO EN LA PROTECCIÓN DE DATOS Y CONSULTA PREVIA

El Encargado ayudará al Responsable con cualquier evaluación de impacto en la protección de datos y consultas previas con autoridades de supervisión u otras autoridades competentes en materia de privacidad de datos que el Responsable considere razonablemente necesarias conforme a cualquier ley de protección de datos relevante.

Dicha asistencia incluirá, cuando sea apropiado, proporcionar al Responsable la información y documentación necesarias.

## MANTENIMIENTO DE REGISTROS

El Encargado mantendrá registros de todas las categorías de actividades de procesamiento realizadas en nombre del Responsable, que contengan:

- El nombre y los datos de contacto del Encargado y de cada Responsable en nombre del cual el Encargado está actuando y, cuando sea aplicable, del representante del Responsable o del Encargado y del oficial de protección de datos.
- Las categorías de procesamiento realizadas en nombre de cada Responsable.
- Cuando sea aplicable, transferencias de datos personales a un tercer país o a una organización internacional, incluyendo la identificación de ese tercer país o aquella organización internacional y, en el caso de transferencias referidas en leyes de protección de datos aplicables, la documentación de las salvaguardias adecuadas.
- Una descripción general de las medidas de seguridad técnicas y organizativas a las que se refiere este Acuerdo.

## DERECHOS DE AUDITORÍA

El Encargado pondrá a disposición del Responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en este Acuerdo y permitirá y contribuirá a auditorías, incluyendo inspecciones realizadas por el Responsable u otro auditor mandatado por el Responsable. Esta auditoría podrá realizarse al menos dos veces al año por el Responsable o un tercero contratado para estos fines.

El Encargado informará de inmediato al Responsable si, en su opinión, una instrucción infringe las leyes de protección de datos aplicables.

## DEVOLUCIÓN O ELIMINACIÓN DE DATOS PERSONALES

Al término del contrato, el Encargado, dentro de los 30 días siguientes a la finalización de los servicios, a elección del Responsable, eliminará o devolverá todos los datos personales al Responsable y eliminará las copias existentes, a menos que la ley aplicable requiera el almacenamiento de los datos personales.

## LEGISLACIÓN APLICABLE Y JURISDICCIÓN

Este Acuerdo se regirá e interpretará de acuerdo con las leyes DEL PAÍS EN QUE SE VENDIERON LOS BIENES O SE PROPORCIONARON LOS SERVICIOS POR PARTE DEL PROVEEDOR.

Cualquier disputa que surja o esté relacionada con este Acuerdo estará sujeta a la jurisdicción exclusiva de los tribunales del respectivo país.El Encargado cooperará con el

Responsable para cumplir con las obligaciones del Responsable bajo las leyes de protección de datos aplicables.

EN TESTIMONIO DE LO CUAL, las partes del presente han ejecutado este Acuerdo a partir de la Fecha de Vigencia. CON LA ACEPTACIÓN DE LA ORDEN DE SERVICIO Y/O ORDEN DE COMPRA, EL PROVEEDOR RECONOCE Y ACEPTA LOS TÉRMINOS Y CONDICIONES CONTENIDOS EN ESTE DOCUMENTO LEGAL VINCULANTE.ESTE DOCUMENTO ES UNA PARTE INTEGRAL DE CUALQUIER ORDEN DE COMPRA Y/O SERVICIO EN EL QUE CONCENTRIX Y EL PROVEEDOR SON PARTES.

## b. English

**DATA PROTECTION AGREEMENT**
**SUPPLIERS**

This Data Protection Agreement ("Agreement") is made as an amendment to the existing contractual relationship between **CONCENTRIX** (Data Processor), including its affiliated companies, and ANY **SUPPLIER** THAT PROVIDES GOOD AND/OR SERVICES in which they are processing personal data, jointly referred to as the "Parties".

**WITH THE ACCEPTANCE OF THE SERVICE ORDER AND/OR PURCHARSE ORDER, THE PROVIDER ACKNOWLEDGE AND ACCEPT THE TERMS AND CONDITIONS CONTAINED IN THIS LEGAL BINDING DOCUMENT.**

Effective Date:

Effective date of the acceptance of the purchase order and/or service order/ or express acceptance of our Policies, Manuals and/or Binding Corporate Rules, or any other legal binding document between parties.

**PURPOSE**

This Agreement outlines the responsibilities and obligations of the Processor concerning the processing of personal data on behalf of the Controller, ensuring compliance with data protection legislation across Latin America. This includes, but is not limited to, the various national data protection laws and regulations in each country within the region. The Processor shall be subjected to Concentrix Privacy Policy for Latam and the Caribbean, Data Privacy Manual, and Privacy Binding Corporate Rules. The documentation can be located here:
The Processor is committed to assisting the Controller in obtaining and maintaining the necessary consent from data subjects for the processing of their personal data. This includes ensuring that data subjects are adequately informed about the purposes of the data

processing, their rights under applicable data protections laws, and any other information necessary to ensure informed consent.

## DEFINITIONS

Personal Data: Any information relating to an identified or identifiable natural person.
Sensitive Personal Data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.
Public Data: Information that is lawfully made available to the public from federal, state, or local government records or other publicly accessible sources.
Private Data: Personal data that is not publicly available and includes information such as names, addresses, social security numbers, and other identifiers.
Financial Data: Personal data related to an individual's financial status, including but not limited to bank account details, credit card information, financial statements, and income information.
Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means.
Data Subject: An individual whose personal data is processed.
Controller: The entity which determines the purposes and means of the processing of personal data.
Processor: The entity which processes personal data on behalf of the controller.
Consent: Any freely given, specific, informed, and unambiguous indication of the data subject’s wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.

## SCOPE AND APPLICATION

This Agreement applies to all personal data processed by the Processor on behalf of the Controller, including private data, public data, sensitive data, and financial information.

This Agreement serves as an amendment to the existing contract between the Controller and the Processor, incorporating data protection requirements as stipulated by relevant legislation across Latin America.

## COMPLIANCE WITH DATA PROTECTION LAWS

The Processor shall comply with all applicable data protection laws and regulations, including but not limited to:

Brazil: Lei Geral de Proteção de Dados (LGPD)

Argentina: Ley de Protección de los Datos Personales
Mexico: Ley Federal de Protección de Datos Personales en Posesión de los Particulares
Colombia: Ley Estatutaria 1581 de 2012
Chile: Ley sobre Protección de la Vida Privada
Peru: Ley de Protección de Datos Personales
Nicaragua: Ley de Protección de Datos Personales
Guatemala: Ley de Protección de la Vida Privada y Datos Personales
Costa Rica: Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales
Jamaica: Data Protection Act
República Dominicana: Ley sobre Protección de Datos de Carácter Personal
The Processor shall assist the Controller in ensuring compliance with these laws, including but not limited to data subject rights requests, data protection impact assessments, and breach notifications.

## DATA PROCESSING INSTRUCTIONS

The Processor shall process personal data only on documented instructions from the Controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by applicable law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

The Processor shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

The Processor shall not process personal data in a manner inconsistent with the Controller's instructions.

## DATA SECURITY

The Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including but not limited to:

Pseudonymization and encryption of personal data.
The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The Processor shall notify the Controller without undue delay after becoming aware of any breach of personal data.

## DATA SUBJECT RIGHTS

The Processor shall assist the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in applicable data protection laws.

The Processor shall promptly notify the Controller if it receives a request from a data subject under any applicable data protection law in respect of personal data processed on behalf of the Controller. The Processor shall not respond to such a request except on the documented instructions of the Controller or as required by applicable laws to which the Processor is subject, in which case the Processor shall inform the Controller of that legal requirement before responding to the request, unless that law prohibits such information on important grounds of public interest.

## DATA BREACH NOTIFICATION

The Processor shall notify the Controller without undue delay after becoming aware of a personal data breach. Such notification shall include:

The nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.
The likely consequences of the personal data breach.
The measures taken or proposed to be taken by the Processor to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

## DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

The Processor shall aid the Controller with any data protection impact assessments and prior consultations with supervisory authorities or other competent data privacy authorities, which the Controller reasonably considers to be required of any relevant data protection law.

Such assistance shall include, where appropriate, providing the Controller with necessary information and documentation.

## RECORD KEEPING

The Processor shall maintain records of all categories of processing activities carried out on behalf of the Controller, containing:

The name and contact details of the Processor and of each Controller on behalf of which the Processor is acting, and, where applicable, of the Controller's or Processor's representative, and the data protection officer.
The categories of processing carried out on behalf of each Controller.
Where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in applicable data protection laws, the documentation of suitable safeguards.
A general description of the technical and organizational security measures referred to in this Agreement.

## AUDIT RIGHTS

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Agreement and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. This audit can be done at least twice a year by the controller, or a third party hired for these purposes.

The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes applicable data protection laws.

## RETURN OR DELETION OF PERSONAL DATA

Upon termination of the contract, the Processor shall, within the 30-days after the termination of the services, at the choice of the Controller, delete or return all the personal data to the Controller and delete existing copies unless applicable law requires storage of the personal data.

GOVERNING LAW AND JURISDICTION

This Agreement shall be governed by and construed in accordance with the laws of THE COUNTRY IN WHICH THE GOOD WAS SOLD OR THE SERVICES WAS PROVIDED BY THE PROVIDER.

Any disputes arising out of or in connection with this Agreement shall be subject to the exclusive jurisdiction of the courts of the respective Country

The Processor shall cooperate with the Controller in meeting the Controller's obligations under applicable data protection laws.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the Effective Date.

WITH THE ACCEPTANCE OF THE SERVICE ORDER AND/OR PURCHARSE ORDER, THE PROVIDER ACKNOWLEDGE AND ACCEPT THE TERMS AND CONDITIONS CONTAINED IN THIS LEGAL BINDING DOCUMENT.

THIS DOCUMENT IS AN INTEGRAL PART OF ANY PURCHARSE ORDER AND/OR SERVICES IN WHICH CONCENTRIX AND THE PROVIDER ARE PARTIES

## c. Portuguese

**ACORDO DE PROTEÇÃO DE DADOS**
**FORNECEDORES**

Este Acordo de Proteção de Dados ("Acordo") é celebrado como uma emenda à relação contratual existente entre a CONCENTRIX (Operador de Dados), incluindo suas empresas afiliadas, e QUALQUER FORNECEDOR QUE FORNEÇA BENS E/OU SERVIÇOS nos quais processam dados pessoais, referidos conjuntamente como as "Partes".

**COM A ACEITAÇÃO DA ORDEM DE SERVIÇO E/OU ORDEM DE COMPRA, O FORNECEDOR RECONHECE E ACEITA OS TERMOS E CONDIÇÕES CONTIDOS NESTE DOCUMENTO LEGALMENTE VINCULANTE**.

**Data de Vigência**:

Data efetiva da aceitação da ordem de compra e/ou ordem de serviço, ou aceitação expressa de nossas Políticas, Manuais e/ou Regras Corporativas Vinculantes, ou qualquer outro documento legalmente vinculante entre as partes.

**OBJETIVO**

Este Acordo estabelece as responsabilidades e obrigações do Operador em relação ao processamento de dados pessoais em nome do Controlador, garantindo a conformidade com a legislação de proteção de dados na América Latina. Isso inclui, mas não se limita, às diversas leis e regulamentos nacionais de proteção de dados em cada país da região. O Operador estará sujeito à Política de Privacidade da Concentrix para a América Latina e o Caribe, Manual de Privacidade de Dados e Regras Corporativas Vinculantes de Privacidade. A documentação pode ser localizada aqui:

O Operador se compromete a auxiliar o Controlador na obtenção e manutenção do consentimento necessário dos titulares dos dados para o processamento de seus dados pessoais. Isso inclui garantir que os titulares dos dados sejam adequadamente informados sobre os propósitos do processamento de dados, seus direitos sob as leis de proteção de dados aplicáveis, e quaisquer outras informações necessárias para garantir o consentimento informado.

## DEFINIÇÕES

- **Dados Pessoais**: Qualquer informação relacionada a uma pessoa natural identificada ou identificável.
- **Dados Pessoais Sensíveis**: Dados pessoais que revelem origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos com a finalidade de identificar exclusivamente uma pessoa natural, dados relativos à saúde, ou dados relativos à vida sexual ou orientação sexual de uma pessoa natural.
- **Dados Públicos**: Informações que são legalmente disponibilizadas ao público por registros de governos federais, estaduais ou locais ou outras fontes acessíveis publicamente.
- **Dados Privados:** Dados pessoais que não estão disponíveis publicamente e incluem informações como nomes, endereços, números de seguridade social e outros identificadores.
- **Dados Financeiros**: Dados pessoais relacionados ao estado financeiro de um indivíduo, incluindo, mas não se limitando a detalhes de contas bancárias, informações de cartões de crédito, demonstrações financeiras e informações de renda.
- **Processamento**: Qualquer operação ou conjunto de operações realizadas sobre dados pessoais, por meios automatizados ou não.
- **Titular de Dados**: Um indivíduo cujos dados pessoais são processados.
- **Controlador**: A entidade que determina as finalidades e os meios do processamento de dados pessoais.

- **Operador**: A entidade que processa dados pessoais em nome do controlador.
- **Consentimento**: Qualquer manifestação livre, específica, informada e inequívoca da vontade do titular dos dados, pela qual ele, mediante declaração ou ação afirmativa clara, concorda com o processamento de dados pessoais que lhe dizem respeito.

## ÂMBITO E APLICAÇÃO

Este Acordo se aplica a todos os dados pessoais processados pelo Operador em nome do Controlador, incluindo dados privados, dados públicos, dados sensíveis e informações financeiras.

Este Acordo serve como uma emenda ao contrato existente entre o Controlador e o Operador, incorporando os requisitos de proteção de dados conforme estipulado pela legislação relevante em toda a América Latina.

## CONFORMIDADE COM AS LEIS DE PROTEÇÃO DE DADOS

O Operador deverá cumprir todas as leis e regulamentos aplicáveis de proteção de dados, incluindo, mas não se limitando a:

- Brasil: Lei Geral de Proteção de Dados (LGPD)
- Argentina: Ley de Protección de los Datos Personales
- México: Ley Federal de Protección de Datos Personales en Posesión de los Particulares
- Colômbia: Ley Estatutaria 1581 de 2012
- Chile: Ley sobre Protección de la Vida Privada
- Peru: Ley de Protección de Datos Personales
- Nicarágua: Ley de Protección de Datos Personales
- Guatemala: Ley de Protección de la Vida Privada y Datos Personales
- Costa Rica: Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales
- Jamaica: Data Protection Act
- República Dominicana: Ley sobre Protección de Datos de Carácter Personal

O Operador deverá auxiliar o Controlador na garantia da conformidade com essas leis, incluindo, mas não se limitando a, solicitações de direitos dos titulares de dados, avaliações de impacto de proteção de dados e notificações de violação.

## INSTRUÇÕES PARA O PROCESSAMENTO DE DADOS

O Operador processará dados pessoais apenas de acordo com as instruções documentadas do Controlador, incluindo no que diz respeito a transferências de dados pessoais para um país terceiro ou organização internacional, salvo se exigido por lei aplicável à qual o Operador está sujeito; nesse caso, o Operador deverá informar o Controlador sobre essa exigência legal antes de processar, a menos que essa lei proíba tal informação por motivos importantes de interesse público.

O Operador deverá garantir que as pessoas autorizadas a processar os dados pessoais tenham se comprometido a manter a confidencialidade ou estejam sob uma obrigação legal adequada de confidencialidade.

## SEGURANÇA DOS DADOS

O Operador implementará medidas técnicas e organizacionais adequadas para garantir um nível de segurança apropriado ao risco.

## DIREITOS DOS TITULARES DE DADOS

O Operador assistirá o Controlador, na medida do possível, no cumprimento da obrigação do Controlador de responder a solicitações para o exercício dos direitos dos titulares dos dados.

## NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS

O Operador deverá notificar o Controlador sem atraso indevido após tomar conhecimento de uma violação de dados pessoais.

## RETORNO OU EXCLUSÃO DE DADOS PESSOAIS

Após a rescisão do contrato, o Operador deverá, dentro de 30 dias após o término dos serviços, excluir ou devolver todos os dados pessoais ao Controlador.

## LEGISLAÇÃO APLICÁVEL E JURISDIÇÃO

Este Acordo será regido e interpretado de acordo com as leis do PAÍS EM QUE O BEM FOI VENDIDO OU O SERVIÇO FOI PRESTADO PELO FORNECEDOR.

Quaisquer disputas decorrentes ou relacionadas a este Acordo estarão sujeitas à jurisdição exclusiva dos tribunais do respectivo País.

O Operador deverá cooperar com o Controlador no cumprimento das obrigações do Controlador de acordo com as leis de proteção de dados aplicáveis.

EM TESTEMUNHO DISSO, as partes abaixo-assinadas executaram este Acordo na Data Efetiva.

COM A ACEITAÇÃO DA ORDEM DE SERVIÇO E/OU ORDEM DE COMPRA, O FORNECEDOR RECONHECE E ACEITA OS TERMOS E CONDIÇÕES CONTIDOS NESTE DOCUMENTO LEGALMENTE VINCULANTE.

ESTE DOCUMENTO É PARTE INTEGRANTE DE QUALQUER ORDEM DE COMPRA E/OU SERVIÇO NO QUAL CONCENTRIX E O FORNECEDOR SEJAM PARTES.

## 14. RESPONSÁVEIS PELA PRIVACIDADE DE DADOS NA AMÉRICA LATINA

**Natalia González Lewis**

LATAM Compliance Manager & Officer

natalia.lewis@concentrix.com

**Juan Andres Trujillo Sanchez**

Data Protection Officer

juan.trujillo@concentrix.com

**Bruno Ricardo Soares**

Data Privacy Analyst

bruno.soares@concentrix.com

## 15. HISTÓRICO DE ALTERAÇÕES

| Versão | Data | Descrição |
|---|---|---|
| 1 | 29/12/2022 | Criação do Manual de Procedimentos para a proteção de dados pessoais. |
| 2 | 24/9/2024 | Correções menores e inclusão de idioma relacionado ao BCR, IA, e a inclusão do Acuerdo General de Proteção de Dados Pessoais para Contratantes. |

## 16. FLUXO DE APROVAÇÃO

| ELABORÓ | REVISÓ | APROBÓ |
|---|---|---|
| **Nombre:** Bruno Soares<br><br>**Cargo**: Analista de privacidad de Datos Concentrix | **Nombre:** Juan Andrés Trujillo Sánchez<br><br>**Cargo**: Oficial de Protección de Datos Concentrix | **Nombre:** Natalia González Lewis<br>**Cargo**: Gerente de Cumplimiento Concentrix |

## INDEX

## 4. AIM

The group of commercial companies that make up the Concentrix group (hereinafter jointly referred to as "Concentrix" and/or "CX" ), recognize the importance of the security, privacy and confidentiality of the personal information that users, clients, suppliers, employees, business partners, candidates and third parties may provide and/or transfer to Concentrix, through the various channels enabled, such as, but not limited to: websites, applications, social networks, physical and/or digital documents.

As a consequence of the above, Concentrix is committed to: (i) the effective protection of the rights of the Owners [6]; and (ii) the adequate Treatment [7]of Personal Data [8], in accordance with the applicable regulations on privacy and protection of personal data.

Therefore, the objective of this Internal Manual on Privacy and Protection of Personal Data (hereinafter the "Manual") is to complement the general provisions of the Personal Data Processing Policy for Concentrix at: https://www.concentrix.com/legal/ and define the general internal guidelines applicable to Concentrix to ensure the application, monitoring, maintenance and continuous improvement of the procedures associated with the processing of personal data in the development of its activities.

## 5. SCOPE

The scope of this Manual is to establish: (i) the procedure for handling PQRs related to the processing of personal data, which will be carried out internally, when Concentrix acts as the data controller; (ii) the procedure for receiving and escalating to our clients PQRs related to the processing of personal data, when Concentrix acts as the data processor (hereinafter "escalation"), and; (iii) the internal procedure in the event of a possible information security incident or "data protection/privacy breach".

This Manual applies in a binding and transversal manner to Concentrix LATAM and the Caribbean and the Caribbean , understood as all its CX subsidiaries and affiliated companies in LATAM and the Caribbean [9]; which are described in section 5 of the Personal Data Processing Policy https://www.concentrix.com/legal/ Therefore, knowledge and proper application of these methods are mandatory for all gamechangers who are part of CONCENTRIX LATAM AND THE CARIBBEAN.

d

## 6. DEFINITIONS

[6] How it is defined below.
[7] Ibid.
[8] Ibid.
[9] CX is made up of companies established in the following countries: United States (only when the client is located in Latin America), Mexico, El Salvador, Guatemala, Honduras, Nicaragua, Costa Rica, Dominican Republic, Jamaica, Colombia, Mexico, Peru, Panama, El Salvador, Nicaragua, Guatemala, Honduras, among others.

This Manual is governed by the following definitions:

6.1. **Database Administrator:** This is the natural person associated with Concentrix, who is assigned, as part of his/her functions, under an employment or service contract, the development of tasks and responsibilities inherent to the Organization's Personal Databases. The Database Administrator is responsible for monitoring the proper application of the Privacy Policies that are applicable to each process and for providing the personal data protection officer and/or the Compliance area with the information required to comply with all legal requirements in this area, such as the periodic registration of databases and their updating.

6.2. **Files or information repositories:** set of documents in physical or digital media, kept by the company, containing personal information regulated by law.

6.3. **Authorization:** Prior, express and informed consent of the Owner to carry out the Processing of Personal Data.

**Note:** In Brazilian legislation there are various legal bases that allow the processing of personal data, which include, in addition to the authorization consent of the owner, another 9 (nine) possibilities[10]

6.4. **Data Protection Authority:** This is the authority in charge in each country of monitoring and supervising that the principles, rights and guarantees of the Data Subjects are respected in the Processing of Personal Data.

6.5. **Privacy Notice:** This is the physical, electronic or any other known or unknown document, which is made available to the Owner in order to inform about the Processing of their Personal Data. The Privacy Notice informs the Owners of the information regarding the existence of the information Processing policies that will be applicable, the way to access them and the characteristics of the Processing that is intended to be given to the Personal Data.

6.6. **Database:** Organized set of Personal Data that is subject to Processing.

6.7. **Successor in title:** Person who through succession or transmission acquires the rights of another person.

6.8. **Authorized Collaborator:** Concentrix Collaborator who is authorized by his or her specific work or functions to access or perform any type of processing on a database managed by Concentrix, which may contain personal data.

6.9. **Personal Data Protection Committee:** Internal body of Concentrix made up of the legal manager, the Compliance manager, the IT Compliance area delegates, the

[10]The above in accordance with art. 7 of Law 13709/2018 – General Law on Personal Data Protection of Brazil (LGPD)

Information Security area delegates and the Personal Data Protection Officer, with the purpose of ensuring the effective implementation of policies and procedures adopted in compliance with the general regime of personal data protection and executing action plans in the event of possible information security incidents that may affect the integrity, confidentiality and/or integrity of personal data.

6.10. **Inquiry:** This is the request made by the Holder regarding his/her Personal Data that is stored in the Concentrix databases and that is not restricted in accordance with the legislation, according to the procedures established in the Comprehensive Personal Data Management Program.

6.11. **Personal Data(s):** Any information linked to or that can be associated with one or more specific or identifiable natural persons.

6.12. **Sensitive data:** Sensitive data is understood to be data that affects the privacy of the Owner or whose misuse may lead to discrimination, such as data that reveals racial or ethnic origin, political orientation, religious or philosophical beliefs, membership in unions, social organizations, human rights organizations or that promote the interests of any political party or that guarantee the rights and guarantees of opposition political parties, as well as data relating to health, sexual life and biometric data.

6.13. **Personal Data Protection Officer and/or Local Data Protection Delegate and/or Leader:** This is the natural person who meets the profile established by law and whose function is to monitor and control the application of the Personal Data Processing Policy.

**Note:** In the regulations applicable in Brazil, the above definition corresponds to the term Data Controller (Encarregado de Proteção de Dados)

6.14. **Escalation:** procedure for escalating requests from data subjects to Concentrix clients, so that they can respond directly.

6.15. **Data Processor/Data Processor:** Natural or legal person, public or private, who by itself or in association with others, carries out the Processing of Personal Data on behalf of the Data Controller.

**Note:** In the regulations applicable in Brazil, the above definition corresponds to the term Operator.

6.16. **Habeas Data (when applicable):** Right of every person to know, update and rectify the information that has been collected about them in public or private files and databases.

6.17. **Security incident or event:** loss, access, unauthorized use and/or theft of Personal Data, violation of the procedures contained in this Manual and in the Concentrix

Privacy and Information Security Policies, unauthorized delivery of information and Personal Data to third parties, unauthorized Processing of Personal Data in accordance with the Concentrix Privacy Policies.

6.18. **Binding Corporate Rules:** This is one of the legal mechanisms established by law that allows the transfer of information within a business group.

6.19. **PQRs:** Term that includes Requests, Complaints, Claims and Suggestions from the owners of the information or those who intend to assert rights related to personal data.

6.20. **Claim:** It is the request made by the Owner regarding his/her Personal Data that is stored in the Concentrix databases, through which he/she may request the deletion of his/her personal data and/or revoke the authorization granted for the Processing of the same.

6.21. **Data Controller/Data Processor:** Natural or legal person, public or private, who by itself or in association with others, decides on the database and/or the processing of data.

**Note:** In the regulations applicable in Brazil, the above definition corresponds to the term: Responsible

6.22. **Subprocessor:** company contracted by the processor/Processor for the processing of personal data.

6.23. **Owner(s):** Natural person whose Personal Data is subject to Processing.

6.24. **Transfer of Personal Data or Personal Databases:** This is the delivery of Personal Data or Personal Databases by a Data Controller to another natural or legal person so that the latter may act on its own behalf as Data Controller of the Personal Data or Databases received.

6.25. **Transmission of Personal Data:** It is the delivery of Personal Data or Personal Databases by a Data Controller to another natural or legal person so that the latter, in its capacity as Data Processor, carries out the Processing of Personal Data on behalf of the person who delivers it in accordance with the obligations established in the contract entered into for this purpose.

6.26. **Processing:** Any operation or set of operations on Personal Data, such as collection, storage, use, circulation or deletion.

6.27. **Personal Data Security Incident:** Any breach of security that results in the accidental or unlawful destruction, loss or alteration of Personal Data held or processed, or unauthorized communication or access to such data.

6.28. **Information Holders:** Clients, Suppliers, Subcontractors, Visitors, Collaborators or Employees of Concentrix, who have provided the information or Personal Data by virtue of the service provided by it.

# 4. PRELIMINARY CONSIDERATIONS

## 4.1 Collection of personal data and consent of the owner

The Authorized Collaborator for the collection of personal data must request and keep a record in a secure medium of the authorization for the processing of personal data of the owner of the information, unless the applicable law on the processing of personal data provides that this is not required.

Prior to carrying out any type of Personal Data Processing (capture or collection, use, storage, circulation, transmission, transfer, updating, modification, deletion, among others), the Authorized Collaborator must verify that the personal data to be provided are strictly necessary to fulfill the purposes for which they are required and that are established in the Concentrix Privacy Policy.

The Authorized Collaborator may not carry out Personal Data Processing in isolation, in documents or manuscripts that are not part of the respective Database, which will be reported to the Compliance area and to the personal data protection officer.

When the collection of information is done through non-face-to-face means, such as the website, mobile application and/or Call center, the evidence of the authorization for the Collection and Processing of Personal Data by the Owner will be recorded in the system used by the non-face-to-face means (Example: on the website and mobile application, the proof is generated by clicking on the "Accept" box of the check-box, when accepting the Privacy Policies; likewise, in the Call Center, proof of authorization can be kept in the recording of the call).

If it is not possible to make the Privacy Policies and the purposes of the processing available to the Data Subjects, Privacy Notices must be posted in visible and easily accessible places, physically or digitally, in the physical locations or websites where personal data is collected.

## 4.2 Creation and/or modification of databases

Concentrix has Databases previously identified by the data governance area, whose control is headed by the Personal Database administrators within the Organization. This process must have support and guidance from the Compliance area and the Personal Data Protection Officer.

Whenever a new database is created or any modifications to existing Personal Databases, approval must be obtained from the data governance area and the area and/or delegate within the organization for the Protection of Personal Data through an authorization request sent to the following email addresses: proteccion.dedatos@concentrix.com and proteccion.dedatos@Concentrix.com in order to maintain the traceability of the information repositories and databases and make the corresponding report to the personal data protection authorities when applicable.

## 4.4 Appropriate storage of personal data

- Regardless of the means of collecting personal data, whether physical or digital, the corresponding consent of the data owner must be requested and kept under adequate security conditions, and in accordance with the parameters established in Concentrix's Personal Data Processing Policy.

- Personal Data must be stored in Databases or information repositories that comply with the security measures defined in the Information Security Policy available for consultation on the Isolución document management platform as: SI-TRS-006 INFORMATION SECURITY.

- Physical databases must comply with appropriate security measures in order to prevent unauthorized consultation, alteration and/or loss of personal information.

- For the processing of documents containing personal data, Concentrix's guidelines and procedures for document management must be followed.

## 4.4 Circulation of Personal Data

- Collaborators and/or related third parties may share Personal Data with other Collaborators, authorized related third parties and/or areas of the Organization when this is necessary for the performance of their duties, in accordance with the responsibilities of their position. However, this Processing of personal information must be carried out in strict compliance with the purposes of the processing of the information collected and in accordance with the provisions of Concentrix's Privacy Policies.

- It is prohibited and considered a serious offense for Collaborators and/or related third parties to circulate, transfer, transmit, send, share and/or communicate personal information of Data Subjects to collaborators who are not authorized to access it or to third parties outside of Concentrix. If a collaborator becomes aware of a possible information leak, he/she must contact the ethics line and inform the Compliance area and the personal data protection officer.

- When a collaborator receives a request that involves the delivery of personal data, whether from an Authority or an individual, this must be channeled to the Compliance area and/or the Personal Data Protection officer in order to evaluate it and provide a response in accordance with the procedure described in sections 4 to 6 of this Manual.

- For any questions or queries regarding the use and circulation of Personal Data in relation to the purpose for which it was collected, or regarding the processing of

personal data in general, employees may contact the Compliance department or the personal data protection officer.

## 4.5 Transfer and Transmission of Personal Data Collected

Concentrix may Transfer (Controller to Controller) or Transmit (Controller to Processor) Personal Data held in the Organization's databases, provided that the Data Subject is informed of such purpose and the safeguards established in the applicable law for the Transfer and/or Transmission of Personal Data are complied with. If the Transmission is made to third parties located in different countries, an international personal data transmission contract must be entered into with that Processor or the applicable legal safeguard will be applied, as the case may be.

## 4.6 Processing of Personal Data of Children and Adolescents

The Processing of Personal Data of children and adolescents will be carried out exceptionally, taking into account the purposes of the processing of the data, respect for their fundamental rights and their best interests and their right to be heard beforehand. Likewise, the authorization of the person who has their parental authority or their legal representative will be required.

The Collaborator and/or third party in charge who, by virtue of their functions, has knowledge of Personal Data of children and adolescents, must have special protection and the Processing of this data requires the implementation of greater security and care measures.

## 4.7 Processing of Sensitive Data

The collaborator and/or third party in charge who, due to their functions, must process sensitive data must exercise greater diligence to safeguard its integrity, confidentiality and security. Therefore, the processing of sensitive data may only be carried out when the applicable law so permits and with the express authorization of the owner of the information, except for exceptions provided by law.

# 5. GOOD PRACTICES FOR RESPONDING TO REQUIREMENTS AND PQRs

In order to process any request or PQR, the following steps must be followed:

5.2. Identify the object of the Request in order to provide a direct, clear and concrete response. When new Databases containing Personal Data are generated, the area in charge must ensure compliance with the provisions of Concentrix's Information Security and Document Management Policies and Procedures.

5.2. Mention the facts that allow a logical understanding of the answers.

5.3 Make precise reference to documents that are sent or delivered as attachments, so that there is a causal link between the Request and the responses.

5.3. State in a concrete manner the legal, technical and/or contractual justifications that are applicable or necessary.

5.4. When there are situations that can be improved and/or corrected, report the measures that are being studied or that will be adopted.

5.11. Ensure that the response does not cause reprocessing or reiterations by the Competent Authority or by the holder

5.12. At the end of each response, include the corresponding annexes or files, briefly indicating their purpose and stating their content or name, duly paginated.

5.13. Refrain from sending information and documents that are not requested or that are not directly related to the Request.

5.14. Document the response to all Requests (whether verbal, physical or electronic), through the respective filing

5.15. Keep a copy of the response to the Request and its respective annexes in a safe place.

5.16. When the Requirements of the holder or the Competent Authorities are not clear or contain formal inaccuracies that may affect the response, contact the Competent Authority with sufficient notice before the deadline, in order to clarify the points in question, without exceeding the maximum legal time to respond to the requirement.

# 6. PROCEDURE FOR HANDLING REQUIREMENTS FROM COMPETENT AUTHORITIES

Collaborators in charge of receiving, responding to and sending requests must follow the following procedure to respond to requests from competent authorities, regardless of the type of Request:

## 6.1. Reception of the Competent Authority Request or PQR

In the event that a Concentrix employee receives a Request related to personal data or requesting any type of personal data through any reception channel, he/she must, within a period of no more than one (1) business day, communicate and notify, as appropriate, to the email address: proteccion.dedatos@concentrix and/or

proteccion.dedatos@concentrix.com, to the personal data protection officer/Compliance area and to his/her immediate superior.

Failure to comply with this duty may be considered a serious offence.

## 6.2. Sending the request to the responsible area

Once the Request has been received, the area or department assigned by Concentrix for said reception must establish and identify the type of request and its object, in order to direct it to the area responsible for responding.

In order to determine the area or department of Concentrix that must respond to the Requirement, the following criteria must be taken into account:

| Type of Requirement | Area or Department Responsible for Responding to the Request | Contact Information |
|---|---|---|
| Requirements related to prevention, investigation and punishment of acts of corruption. | Compliance Department | Email: natalia.lewis @concentrix.com |
| Requirements related to occupational risks and occupational health | Human Resources Department | E-mail: relations.laborales.co@onelinkbpo.com |
| Requirements related to the handling of personal data | Privacy Department / Personal Data | E-mail: proteccion.dedatos@concentrix.com and juan.trujillo@concentrix.com |
| Requirements related to issues of unfair competition, restrictive practices and intellectual property. | Legal Department | E-mail: juliancamilo.diaz @ concentrix.com |
| Requirements related to e-commerce and consumer protection issues | Legal Department | E-mail: juliancamilo.diaz @ concentrix.com |

## 6.3 Determining whether Concentrix is competent

In the event that Concentrix is not competent, because it is not the appropriate subject to respond to the Request, it must immediately inform the Competent Authority, if it acts verbally, or within two (2) business days following receipt, in the event that the Request has been received in writing or electronically.

## 6.4 Determine whether the application is complete or whether additional information or support should be requested

In the event that the request is not clear or is incomplete, clarification will be requested from the requesting authority as soon as possible and within a maximum of two (2) business days following the date of receipt, and once the required information is received, the request will be immediately responded to, in order to comply within the term established by the competent authority.

## 6.5 Establish whether the Request involves personal data or confidential or reserved information of Concentrix

Where the Request involves disclosing or providing confidential or reserved information, Concentrix shall indicate this to the Competent Authority in its response to the Request.

Likewise, when it comes to personal data of information holders, which are subject to processing by Concentrix, once prepared by the area in charge of providing the information, the request must be reviewed by the Compliance area and by the Concentrix personal data protection officer to approve the response and verify that it complies with the requirements of the regulations on the processing of personal data.

Information holders are understood to be those natural or legal persons who are contractors, clients, suppliers or business partners of Concentrix, about whom confidential or reserved information is processed, which may be requested in a Request.

## 6.6 Preparation of the response to the request

The response to the request will be made by the Concentrix area in charge of providing the required information. The response must meet the following requirements: i) timely, ii) objective, iii) truthful, iv) complete, v) motivated and vi) up to date.

- It is appropriate when it is filed within the time limits stipulated by law or in the Request.

- It is objective when it is answered based on the content of the documents and evidence that are attached.

- It is true when its content is verifiable according to the documents and evidence attached.

- It is complete when each of the questions and/or requests of the Requirement are answered.

- It is motivated when there is justification for the different provisions included in the response to the Request.

- It is updated when it is based on recent information and data.

- In cases where the Requirements have different requests or questions, these must be answered in the same order in which they are requested and in a clear manner.

## 6.7 Sending the response

- Regardless of the medium in which the Request was received, the response will be sent in writing, either electronically (such as email) or physically, as indicated by the Competent Authority.

- The response to the Request must be sent to the physical or electronic address stated in the request or in the official media of the authority that made the request.

- The response to the Request must be addressed to the Competent Authority and to the official who made the request.

- For the purposes of proving shipment, the receipt and the filing number of the Requirement must be kept.

## 6.8 Term to respond to the Competent Authority Request

Unless otherwise provided for by a special rule or provision, Requests must be resolved within the period stated in the request. When, exceptionally, it is not possible to resolve the Request within the period indicated above, Concentrix, through the competent area or department in charge of responding and/or to which the Request was addressed, must inform the Competent Authority of this circumstance, stating the reasons for the delay and indicating a reasonable period within which the Request will be resolved or responded to.

# 7. PROCEDURE FOR RESPONDING TO PQRs FROM INFORMATION OWNERS

This procedure only applies when Concentrix acts in its capacity as Controller of the processing of personal data, since when it acts as a processor, as a general rule the "Escalation" procedure previously established with the client must be followed to transfer the PQRs to them and for them to respond directly.

## 7.1. When Concentrix is responsible for personal data

Concentrix users, clients, suppliers, employees or applicants have the right to know the details of the processing of their personal data and to exercise their rights as Data Owners,

through queries, requests and complaints under the terms of the data protection regulations applicable to them and as established in this Privacy Policy.

For the purposes of the above, this Manual defines the general procedure for the exercise of rights by the Holders of the information, without prejudice to the application of specific procedures and requirements that the local laws of each territory may contemplate. In the event of a discrepancy between the general procedure established in this Manual and the specific procedures or requirements contained in the applicable local regulations of each territory, the latter shall prevail.

### 7.1.1 Reception of PQR'S (MAIL, WINDOW, FAX AND/OR E-MAIL).

Applications may be submitted in writing, physically and/or digitally, and through the channels enabled by the Organization for this purpose, which are:

viii) In person, either verbally or in writing, in the physical spaces designated by Concentrix for such purposes, such as the offices located at: Calle 63 # 24 – 80, in Bogotá - Colombia

ix) By phone, at the phone number: (+57) 4 444 38 20

x) By physical or postal mail, which depending on the corresponding country will be:

To the email: proteccion.dedatos@concentrix.com

In the event that a Concentrix employee receives a Request related to personal data through reception channels other than those mentioned in this section, he/she must, within a period of no more than one (1) business day, communicate and notify it, as appropriate, to the following email address: to the personal data protection officer/Compliance area and to his/her immediate superior.

Failure to comply with this duty may be considered a serious offence.

### 7.1.2. Determine whether Concentrix is competent

Once the Request is received, the Compliance area or the Personal Data Protection Officer will determine whether Concentrix is competent to resolve the request.

In the event that Concentrix is not competent, it must inform the owner or interested party within two (2) business days following receipt (unless otherwise agreed upon which a different term is established in the contract or in another document signed with the client).

### 7.1.3 Determine whether the applicant is entitled to make the request

It is essential to determine whether the person requesting the data is entitled to make the request; this will depend on the applicable legislation, but as a general rule the requester must be: i) the data owner, or ii) his legal representative, or iii) a person duly authorized by the owner to make the query or claim, or iv) his legal heir, given that providing personal information, modifying it or deleting it when it is not the person entitled by law to do so may result in a violation of the protection of personal data and negatively affect Concentrix. Therefore, the following must be taken into account:

- The Owner of the information and/or the person exercising the right on his/her behalf must prove his/her Ownership in order to avoid loss, consultation, unauthorized or fraudulent use or access by a person other than the Interested Party and/or who does not have a legal mandate to act on his/her behalf.

- The accreditation by the Holder will be provided by sending: a physical or digital copy of the relevant identification document according to the means of submitting the query.

- When the request is made by a person other than the Owner, the third party must duly prove the legal status or mandate to act on behalf of the Owner by sending the supporting documents.

The request will be managed by the area and/or delegate in charge within the organization for the protection of personal data only when Ownership can be accredited and the previously mentioned requirements are met.

### 7.1.4 Determine whether the application is complete or whether additional information or support should be requested

The request to exercise any of the aforementioned rights must contain at least the following information:

- Name of the Interested Party, his/her representative and/or the person exercising the right on his/her behalf, and identification number.

- Specific, precise and justified request for consultation and the right invoked.

- Physical and/or electronic address for notifications.

- Documents supporting the application (if applicable)

- Signature of the petitioner according to the means of the request.

If the application is incomplete, the interested party will be required within five (5) business days following the date of receipt to correct the deficiencies.

The requested information must be submitted by the applicant within two (2) months following the request; failure to do so will be deemed to have resulted in the applicant having withdrawn.

The request will be managed by the area and/or delegate in charge within the organization for the protection of personal data only when Ownership can be accredited and the previously mentioned requirements are met.

### 7.1.5 Request redirection

If it is determined that Concentrix is competent to respond, a determination will be made as to whether the request is of a technical or legal nature or whether it has a technical and legal part, in order to direct it to the area responsible for responding.

If the request is entirely of a legal nature, it will be resolved directly by the Compliance department or the Personal Data Protection Officer; otherwise, support will be requested from the Information Security department and/or the department in charge of responding to the request.

### 7.1.6 Preparation of the response to the request

The response to the request must be timely, objective, truthful, complete, motivated and up to date.

- It is appropriate when it is filed within the time limits stipulated by law or in the Request.
- It is objective when it is answered based on the content of the documents and evidence that are attached.
- It is true when its content is verifiable according to the documents and evidence attached.
- It is complete when each of the questions and/or requests of the Requirement are answered.
- It is motivated when there is justification for the different provisions included in the response to the Request.
- It is updated when it is based on recent information and data.
- In cases where the Requirements have different requests or questions, these must be answered in the same order in which they are requested and in a clear manner.

### 7.1.7 Sending the response

- Regardless of the medium in which the Request was received, the response will be sent in writing, either electronically (such as email) or physically, as indicated by the Competent Authority.

- The response to the Request must be sent to the physical or electronic address indicated by the owner of the information or the interested applicant.

- The response to the Request must be addressed to the applicant who made the request.

- For the purposes of proving shipment, the receipt and the filing number of the Requirement must be kept.

### 7.1.8 Term to respond to PQRs from personal data holders

The maximum term that Concentrix has to respond to the request is fifteen (15) business days counted from the day following the date of receipt. When it is not possible to respond to the request within said term, the interested party will be informed of the reasons for the delay and the date on which the request will be responded to, which may not exceed eight (8) business days following the expiration of the first term.

## 7.2 When Concentrix is responsible for personal data (Escalation)

When Concentrix receives PQRs from holders and in relation to their personal data and acts solely as the person in charge of the information, it forwards the requests it receives to the person responsible for the information through the Escalation procedure, so that the client can respond directly to the petitioners/holders of the information.

The Escalation procedure and contact details for escalating requests and queries from data subjects must be agreed in advance and described in the agreements that Concentrix signs with the client at the time of initiating its contractual relationship.

- Prepare an escalation script for the processing of personal data that includes general guidelines on how to direct a PQR through the channels available to the person responsible for processing personal data.

- Request approval from the data controller regarding the escalation script.

- Disseminate the escalation script with operational training areas for its implementation.

# 8. SECURITY MEASURES AND SECURITY INCIDENTS

## 8.1 Security Measures

Concentrix has defined and implemented the relevant security measures for the protection of the Personal Information of all our clients, collaborators, suppliers and shareholders , which have been established based on international standards and regulations, such as ISO27001:2013, PCI-DSS (Credit Card Information Security Standard) and SOX (Sarbanes-Oxley Act).

Security measures are established in the Information Security Policy, as well as in the Specific Policies and Procedures and Security Standards cited below:

- Information Security Policy
- Incident Management Policy
- Cryptography Policy
- Information Asset Management Policy
- Access Management Policy
- Security Policy in Operations

## 8.2 Events of non-compliance with the Privacy Policies, Information Security Policy and applicable Standards

In the event of a possible Security Incident regarding the Processing of Personal Data, this must be reported to the area and/or delegate within the Organization for the Protection of Personal Data at the email address: proteccion.dedatos@concentrix.com by the collaborator or collaborators who have had knowledge of it, immediately after its occurrence, in order to begin the pertinent investigation, the action plan and corrective measures, and the respective report to the internal areas and competent authorities, within the terms established by the Law, if applicable.

# 9. RESPONSIBILITY FOR THE PROCESSING OF CONCENTRIX DATABASES

Each of the areas and collaborators that manage personal data in the performance of their duties are responsible for the proper management of the databases and other information repositories that contain personal data, and for complying with Concentrix's policies and procedures regarding the processing of personal data, information security and document management. Likewise, they have the duty to promptly and completely deliver the information required by the Compliance area and/or the personal data protection officer and to collaborate with these areas to facilitate compliance with the legal requirements in this area.

# 11. PENALTIES FOR NON-COMPLIANCE IN THE PROCESSING OF PERSONAL DATA

## 10.1 Sanctions on Concentrix

The sanctions that may be imposed by the competent authorities on Collaborators and Concentrix vary depending on the applicable regulations according to the country or countries in which the Personal Data Protection Obligations are breached, which may consist of, but are not limited to:

- Fines of a personal and institutional nature that may be successive as long as the non-compliance that gave rise to them continues.

- Suspension of activities related to the Processing of Personal Data. The corrective measures to be adopted will be indicated in the act of suspension.

- Temporary closure of operations related to the Processing of Personal Data once the suspension period has elapsed without the corrective measures ordered by the competent authority having been adopted.

- Immediate and definitive closure of the operation involving the Processing of Sensitive Data.

## 10.2 Sanctions for collaborators

In the event of non-compliance with the Personal Data Protection policies and procedures established in this Manual, Concentrix contemplates administrative sanctions for all collaborators, which, according to their responsibility in the act and the seriousness of the non-compliance, may lead to the termination of the contractual relationship. Likewise, the Ethics Committee, in order to ensure compliance with the CNX Code of Ethics and Standards of Conduct, has the function of knowing, analyzing, evaluating, processing, deciding and notifying violations, complaints and claims regarding the protection of personal data.

Collaborators who have access to personal information by virtue of their duties at Concentrix are obliged not to disseminate, comment on, copy, deliver, communicate, give access to, exchange or market in any way or by any means their username and/or password and/or other access credentials to the systems and platforms, whether those of Concentrix, the client, or third parties, that have been made available to them, as well as any personal information of clients, end consumers, employees, co-workers, and any other personal data that they receive or learn about on the occasion of or for the performance of their duties. Likewise, they have the duty to adopt the appropriate security measures and to immediately report any theft, alteration or loss of their credentials, confidential information or personal data, immediately when they become aware of it. Failure to comply with this legal and contractual obligation will result in disciplinary, civil and/or criminal sanctions, as appropriate

## 11. DATA PROTECTION OFFICERS IN THE LATAM REGION


## 12. USE OF ARTIFICIAL INTELLUGENCE AND PERSONAL DATA

Concentrix, committed to technological evolution to improve the services of our clients and the experience of our employees, shareholders, users and in general any owner of the information, has adopted the development and use of Artificial Intelligence technologies under the declaration of ethical use and principle regarding artificial intelligence of Concentrix: https://www.concentrix.com/wp-content/uploads/2024/04/Concentrix-Generative-AI-Statement.pdf .

Therefore, Concentrix will take into account the declaration of principles for the protection of processed personal data when implementing and developing AI technology. It will also have the following guiding principles: (i) Privacy by Design and by Default; (ii) the Principle

of Minimization of Personal Data, and; (iii) The obligations imposed by current regulations on Artificial Intelligence where we have a commercial presence.

Concentrix is committed to the responsible and ethical use of any technological advance, especially in relation to the comprehensive protection of personal data for which we are responsible and/or in charge.

## 14 BINDING CORPORATE RULES – REFERENCE TO CONCENTRIX DATA PROTECTION MANUAL.

The Binding Corporate Rules ("BCR" and/or "BCR"), regarding data protection, are mandatory for the Concentrix business group when the companies that make up the group transfer, or set of transfers, of personal data to another person in charge within a jurisdiction where Concentrix operates, or to another country where the company also operates.

For this purpose, Concentrix, in compliance with the personal data protection regulations of the jurisdictions where it has a presence in Latin America and the Caribbean, has implemented a compendium of Binding Corporate Rules on the protection of personal data, which have been included in our Manual of Binding Corporate Rules, which can be found at: https://www.concentrix.com/legal/ in the GEO Level Policies section and LATAM subsection.

Within our Manual you will find all of Concentrix's BCRs applicable to the transfer of personal data and other privacy-related aspects.

## 15. GENERAL DATA PROTECTION AGREEMENT FOR CONTRACTORS.

Pursuant to the regulatory requirements regarding the protection of personal data in the jurisdictions in which we have a commercial presence, and the interest of the Concentrix Group in generating confidence in our data subjects regarding the contractual measures established to protect their personal data, we have developed a General Data Protection Agreement for Concentrix Contractors, which establishes in a standard way the contractual, organizational, administrative, human and technical measures that Contractors, who provide services involving the processing of personnel and/or shareholder data, must comply with in order to provide services to Concentrix.

In this way, each Contractor, by completing and signing the supplier forms, service orders, purchase orders, acceptance letters, offer letters and any binding commercial document between Concentrix and the Contractor, expressly and unequivocally accepts the content of the General Data Protection Agreement for Contractors, which will be Annex 1 of this Manual in both Spanish and English.

## DATA PROTECTION AGREEMENT
## SUPPLIERS

This Data Protection Agreement ("Agreement") is made as an amendment to the existing contractual relationship between **CONCENTRIX** (Data Processor), including its affiliated companies, and ANY **SUPPLIER** THAT PROVIDES GOOD AND/OR SERVICES in which they are processing personal data, jointly referred to as the "Parties".

**WITH THE ACCEPTANCE OF THE SERVICE ORDER AND/OR PURCHARSE ORDER, THE PROVIDER ACKNOWLEDGE AND ACCEPT THE TERMS AND CONDITIONS CONTAINED IN THIS LEGAL BINDING DOCUMENT.**

Effective Date:

Effective date of the acceptance of the purchase order and/or service order/ or express acceptance of our Policies, Manuals and/or Binding Corporate Rules, or any other legal binding document between parties.

### PURPOSE

This Agreement outlines the responsibilities and obligations of the Processor concerning the processing of personal data on behalf of the Controller, ensuring compliance with data protection legislation across Latin America. This includes, but is not limited to, the various national data protection laws and regulations in each country within the region. The Processor shall be subjected to Concentrix Privacy Policy for Latam and the Caribbean, Data Privacy Manual, and Privacy Binding Corporate Rules. The documentation can be located here:
The Processor is committed to assisting the Controller in obtaining and maintaining the necessary consent from data subjects for the processing of their personal data. This includes ensuring that data subjects are adequately informed about the purposes of the data processing, their rights under applicable data protections laws, and any other information necessary to ensure informed consent.

### DEFINITIONS

12. Personal Data: Any information relating to an identified or identifiable natural person.
13. Sensitive Personal Data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

14. Public Data: Information that is lawfully made available to the public from federal, state, or local government records or other publicly accessible sources.
15. Private Data: Personal data that is not publicly available and includes information such as names, addresses, social security numbers, and other identifiers.
16. Financial Data: Personal data related to an individual's financial status, including but not limited to bank account details, credit card information, financial statements, and income information.
17. Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means.
18. Data Subject: An individual whose personal data is processed.
19. Controller: The entity which determines the purposes and means of the processing of personal data.
20. Processor: The entity which processes personal data on behalf of the controller.
21. Consent: Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.

## SCOPE AND APPLICATION

This Agreement applies to all personal data processed by the Processor on behalf of the Controller, including private data, public data, sensitive data, and financial information.

This Agreement serves as an amendment to the existing contract between the Controller and the Processor, incorporating data protection requirements as stipulated by relevant legislation across Latin America.

## COMPLIANCE WITH DATA PROTECTION LAWS

The Processor shall comply with all applicable data protection laws and regulations, including but not limited to:

12. Brazil: Lei Geral de Proteção de Dados (LGPD)
13. Argentina: Ley de Protección de los Datos Personales
14. Mexico: Ley Federal de Protección de Datos Personales en Posesión de los Particulares
15. Colombia: Ley Estatutaria 1581 de 2012
16. Chile: Ley sobre Protección de la Vida Privada
17. Peru: Ley de Protección de Datos Personales
18. Nicaragua: Ley de Protección de Datos Personales
19. Guatemala: Ley de Protección de la Vida Privada y Datos Personales

20. Costa Rica: Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales
21. Jamaica: Data Protection Act
22. República Dominicana: Ley sobre Protección de Datos de Carácter Personal

The Processor shall assist the Controller in ensuring compliance with these laws, including but not limited to data subject rights requests, data protection impact assessments, and breach notifications.

## DATA PROCESSING INSTRUCTIONS

The Processor shall process personal data only on documented instructions from the Controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by applicable law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

The Processor shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

The Processor shall not process personal data in a manner inconsistent with the Controller's instructions.

## DATA SECURITY

The Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including but not limited to:

5. Pseudonymization and encryption of personal data.
6. The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
7. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
8. A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The Processor shall notify the Controller without undue delay after becoming aware of any breach of personal data.

## DATA SUBJECT RIGHTS

The Processor shall assist the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in applicable data protection laws.

The Processor shall promptly notify the Controller if it receives a request from a data subject under any applicable data protection law in respect of personal data processed on behalf of the Controller. The Processor shall not respond to such a request except on the documented instructions of the Controller or as required by applicable laws to which the Processor is subject, in which case the Processor shall inform the Controller of that legal requirement before responding to the request, unless that law prohibits such information on important grounds of public interest.

## DATA BREACH NOTIFICATION

The Processor shall notify the Controller without undue delay after becoming aware of a personal data breach. Such notification shall include:

4. The nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.
5. The likely consequences of the personal data breach.
6. The measures taken or proposed to be taken by the Processor to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

## DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

The Processor shall aid the Controller with any data protection impact assessments and prior consultations with supervisory authorities or other competent data privacy authorities, which the Controller reasonably considers to be required of any relevant data protection law.

Such assistance shall include, where appropriate, providing the Controller with necessary information and documentation.

## RECORD KEEPING

The Processor shall maintain records of all categories of processing activities carried out on behalf of the Controller, containing:

5. The name and contact details of the Processor and of each Controller on behalf of which the Processor is acting, and, where applicable, of the Controller's or Processor's representative, and the data protection officer.
6. The categories of processing carried out on behalf of each Controller.
7. Where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in applicable data protection laws, the documentation of suitable safeguards.
8. A general description of the technical and organizational security measures referred to in this Agreement.

## AUDIT RIGHTS

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Agreement and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. This audit can be done at least twice a year by the controller, or a third party hired for these purposes.

The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes applicable data protection laws.

## RETURN OR DELETION OF PERSONAL DATA

Upon termination of the contract, the Processor shall, within the 30-days after the termination of the services, at the choice of the Controller, delete or return all the personal data to the Controller and delete existing copies unless applicable law requires storage of the personal data.

## GOVERNING LAW AND JURISDICTION

This Agreement shall be governed by and construed in accordance with the laws of THE COUNTRY IN WHICH THE GOOD WAS SOLD OR THE SERVICES WAS PROVIDED BY THE PROVIDER.

Any disputes arising out of or in connection with this Agreement shall be subject to the exclusive jurisdiction of the courts of the respective Country

The Processor shall cooperate with the Controller in meeting the Controller's obligations under applicable data protection laws.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the Effective Date.

**WITH THE ACCEPTANCE OF THE SERVICE ORDER AND/OR PURCHARSE ORDER, THE PROVIDER ACKNOWLEDGE AND ACCEPT THE TERMS AND CONDITIONS CONTAINED IN THIS LEGAL BINDING DOCUMENT. THIS DOCUMENT IS AN INTEGRAL PART OF ANY PURCHARSE ORDER AND/OR SERVICES IN WHICH CONCENTRIX AND THE PROVIDER ARE PARTIES.**

## 15. CHANGE HISTORY

| Versión | Date | Description |
|---|---|---|
| 1 | 29/12/2022 | Creation of the Procedures Manual for the protection of personal data. |
| 2 | 24/9/2024 | Minor corrections and inclusion of language related to the BCR, IA, and the inclusion of the General Agreement on the Protection of Personal Data for Contractors |

## 16. APPROVAL FLOW

| PREPARED | REVIEW | APPROVAL |
|---|---|---|
| **Name:** Bruno Soares<br><br>**Position**: DP analyst | **Name:** Juan Andrés Trujillo Sánchez<br><br>**Position**: DPO | **Name:** Natalia González Lewis<br>**Position**: Concentrix Compliance Manager |