POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

TELXIUS CABLE PERÚ S.A.C.

Lima, 1 de enero de 2022

OBLIGACIONES EN MATERIA DE DATOS PERSONALES – TELXIUS CABLE PERÚ S.A.C.

Telxius Cable Perú S.A.C. (en adelante, "Telxius") cumple con las políticas corporativas en materia de protección de datos personales del Grupo Telxius, en concordancia con la regulación de la Unión Europea, previstas en los siguientes documentos:

- Política Global de Privacidad del Grupo Telefónica
- Reglamento del Modelo de Gobierno de la Protección de Datos Personales del Grupo Telxius
- Dominios de desarrollo (Gestión de los derechos de los interesados; Gestión de Terceros; Gestión del Consentimiento y otras bases legitimadoras y Deber de Información; Registro de tratamientos, análisis de riesgo y evaluaciones de impacto; Supresión de Datos de Carácter Personal; Transferencias internacionales; Violaciones de seguridad de datos de carácter personal; Auditoría Interna; Clasificación de Datos; Formación y concienciación)
- Instrucción Global de Medidas de seguridad aplicables a los datos de carácter personal

La regulación peruana en materia de datos personales ha tomado como modelo a la regulación de la Unión Europea. En este sentido, al seguir las políticas y guías aplicables al grupo económico, Telxius es respetuoso de los estándares peruanos en materia de protección de datos personales. Sin perjuicio de ello, el presente documento detalla las buenas prácticas más relevantes adoptadas por Telxius, en cumplimiento de la regulación peruana en materia de protección de datos personales y los documentos más relevantes emitidos por la Autoridad Nacional de Protección de Datos Personales de Perú (en adelante, la "Autoridad de Datos"):

- Ley 29733, Ley de Protección de Datos Personales en Perú (en adelante, la "LPDP")
- Decreto Supremo N° 003-2013-JUS, Reglamento de la Ley (en adelante, el "Reglamento")
- Guía práctica para la observancia del "Deber de Informar"[1]
- El Derecho Fundamental a la Protección de Datos Personales[2]
- Directiva de Seguridad[3]
- Directiva para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia[4]
- Guía de Inscripción de Bancos de Datos Personales[5]

---

[1] Para mayor detalle, ver: https://cdn.www.gob.pe/uploads/document/file/472765/Gu%C3%ADa_Deber_de_Informar.pdf.

[2] Para mayor detalle, ver: https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-Derecho-Fundamentalok.pdf.

[3] Para mayor detalle, ver: https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-de-Directiva-de-Seguridad.pdf.

[4] Para mayor detalle, ver: https://cdn.www.gob.pe/uploads/document/file/523261/Directiva-N_-01-2020-DGTAIPD-1.pdf.

[5] Para mayor detalle, ver: https://cdn.www.gob.pe/uploads/document/file/1401557/Gu%C3%ADa%20de%20%20inscripci%C3%B3n%20de%20bancos%20de%20datos%20personales.pdf.

I. TOMA DE CONSENTIMIENTO

1. Telxius tiene la obligación de recabar el consentimiento de las personas naturales cuyos datos personales trata. El concepto "tratamiento" es bastante amplio, e incluye no solo la utilización efectiva de los datos, sino también la mera posesión o conservación de información.

   Telxius trata datos personales de trabajadores, proveedores (contratas), clientes y visitantes.

2. Sin embargo, de conformidad con las excepciones previstas en la LPDP, Telxius no tiene la obligación de recabar el consentimiento del titular cuando se trata información necesaria para ejecutar una relación contractual o cumplir con la ley.

   Por ello, Telxius no recaba el consentimiento para el tratamiento de datos personales relativos a la ejecución de la relación contractual entre Telxius y sus trabajadores, proveedores (contratas) y clientes.

3. No obstante, cuando dichos datos se utilizan para fines adicionales ajenos a la relación contractual (como lo sería, por ejemplo, utilizar las imágenes de personas para publicitar eventos), Telxius recaba el consentimiento mediante una Cláusula de Usos Adicionales, que detalla lo siguiente:

   - Identificación completa del titular del banco de datos personales y su domicilio;
   - Los usos adicionales para los que será utilizada la información (cada uso adicional es materia de un consentimiento individual para dicho uso en específico);
   - Los datos personales obligatorios para cumplir con la finalidad consignada;
   - Las consecuencias de proporcionar los datos personales y de su negativa a hacerlo;
   - Si realiza transmisión nacional o internacional de datos personales, indicando la identidad de los destinatarios, su ubicación y con qué finalidad se transfieren los datos;
   - Denominación del banco de datos personales que almacena la información proporcionada por el titular de los datos personales.
   - Tiempo de conservación de los datos personales
   - Información relativa al ejercicio de los Derechos ARCO y acerca de la posibilidad de presentar reclamos ante la Autoridad de Datos Personales de considerar que no han sido atendidos en el ejercicio de sus derechos.

   Si entre la información personal se cuenta con "datos sensibles"[6] (por ejemplo, información sobre enfermedades, ingresos económicos, huella digital), el consentimiento se recaba siempre por escrito.

---

[6] **LPDP**
"**Artículo 2.- Definiciones**
Para todos los efectos de la presente Ley, se entiende por:
[…]

4. La autorización que recaba Telxius no implica que otras empresas pueden acceder a dicha información.

   Cuando Telxius requiere que un tercero acceda a los datos personales para fines ajenos a la relación contractual o cumplir con la ley, Telxius recaba el consentimiento del titular mediante el documento legal señalado en el punto *supra*.

   En caso la información se remita a otro agente a fin de que este gestione la información en nombre, interés y bajo el encargo de Telxius, ese agente será un encargado de un banco de datos, y no un tercero, por lo que en este supuesto no se requiere de consentimiento[7].

   Telxius efectúa la transferencia de datos personales a través de encargados que brindan servicios de almacenamiento en la nube con base en el extranjero, lo cual ha sido declarado ante la Autoridad de Datos. Estas empresas cumplen con las medidas de protección de datos personales requeridas.

   En esa línea, Telxius cuenta con cláusulas de Protección de Datos Personales e Indemnidad, que informan a los terceros y encargados los límites dentro los cuales pueden usar la información y que aseguran que mantengan medidas de seguridad suficientes para evitar su pérdida o la violación de su confidencialidad.

5. Por otro lado, para el caso en que Telxius es el receptor de información personal remitida por un tercero (por ejemplo, proveedores y clientes), Telxius cuenta con cláusulas de Protección de Datos Personales e Indemnidad, que aseguran que los terceros cumplen con la normativa en materia de protección de datos personales.

   Ello sin perjuicio de que Telxius verifica que los terceros se encuentren autorizados para efectuar tal flujo de información con la debida diligencia.

---

5. Datos sensibles. *Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual."*

Reglamento de LPDP
"***Artículo 2.- Definiciones***
Para los efectos de la aplicación del presente reglamento, sin perjuicio de las definiciones contenidas en la Ley, complementariamente, se entiende las siguientes definiciones:
[…]
6. Datos sensibles: *Es aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad."*

[7] Según ha referido la Autoridad de Datos en la consulta absuelta mediante Oficio No. 871-2013-JUS/DGPDP del 18 de noviembre de 2013, *"El concepto de responsable del tratamiento sirve para cubrir el supuesto en el que el encargado se limita a ejecutar lo que el titular del banco de datos dispone, en cuyo caso no es "responsable del tratamiento", ya que el "responsable del tratamiento" es siempre el que "decide" sobre el tratamiento."*

II. DEBER DE INFORMAR

6. En todo supuesto de tratamiento de datos personales, Telxius tiene la obligación de poner a disposición del titular de los datos personales toda la información relevante respecto al tratamiento de sus datos personales en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación.

7. Telxius cumple con esta obligación mediante Cláusulas Informativas impresas, que son entregadas a los titulares de los datos personales. En estas cláusulas se cumple con informar los siguientes aspectos sobre el tratamiento:

   - Identificación completa del titular del banco de datos personales y su domicilio;
   - Finalidad del tratamiento de los datos personales;
   - Los datos personales obligatorios para cumplir con la finalidad consignada;
   - Las consecuencias de proporcionar los datos personales y de su negativa a hacerlo;
   - Si realiza transmisión nacional o internacional de datos personales, indicando la identidad de los destinatarios, su ubicación y con qué finalidad se transfieren los datos;
   - Denominación del banco de datos personales que almacena la información proporcionada por el titular de los datos personales;
   - Tiempo de conservación de los datos personales;
   - Información relativa al ejercicio de los Derechos ARCO y acerca de la posibilidad de presentar reclamos ante la Autoridad de Datos Personales de considerar que no han sido atendidos en el ejercicio de sus derechos.

8. Cuando Telxius trata información brindada por terceros, verifica que estos hayan informado sobre la transferencia de dicha información, sea de manera directa o mediante declaraciones expresas, bajo términos de razonabilidad.

III. REGISTRO DE LOS BANCOS DE DATOS EN EL REGISTRO NACIONAL DE PROTECCIÓN DE DATOS PERSONALES

9. La información que se encuentra organizada bajo algún criterio (por ejemplo, sea en un base de datos de Excel o en un archivo de expedientes), califica como un banco de datos (sea éste automatizado o no automatizado[8]).

10. Telxius tiene la obligación de inscribir los bancos de datos personales con los que cuente en el Registro Nacional de Protección de Datos Personales.

11. En ese sentido, Telxius ha inscrito los siguientes bancos de datos ante el Registro Nacional de Protección de Datos Personales:

Titular	Denominación	Código RNPDP-PJP
Telxius	Trabajadores, Cesados y Practicantes	21489
	Proveedores	21490
	Clientes	20547
	Visitantes	20548
	Videovigilancia	20549

[8] Según ha referido la Autoridad de Datos en la consulta absuelta mediante Oficio No. 116-2014-JUS/DGPDP del 05 de marzo de 2014, "[…] *un banco de datos personales no automatizado es el conjunto de datos personales, cuya forma de organización permite acceder rápidamente o mediante esfuerzos razonables a los datos personales que contiene, y se debe analizar cada caso concreto, a la luz de los criterios expuestos* […]. *La experiencia permite incorporar como criterio práctico la posibilidad de diferenciar si estamos frente a un "depósito" de documentos (carente de organización) como un límite objetivo de aquello que "no es" un banco de datos personales."*

IV. REGISTRO DE LOS FLUJOS TRANSFRONTERIZOS

12. La transferencia de datos personales puede ser efectuada hacia receptores situados en el extranjero, en cuyo caso se está frente a un "flujo transfronterizo" de datos personales[9].

13. Todo flujo transfronterizo de datos personales requiere ser comunicado a la Autoridad de Datos para su correspondiente registro.

14. Telxius ha cumplido con declarar el flujo transfronterizo que realiza, mediante la inscripción de los bancos de datos personales señalados ante el Registro Nacional de Protección de Datos Personales.

15. Telxius solo realiza flujo transfronterizo con empresas que cuenten con niveles adecuados de protección de los datos personales, lo que se garantiza a través de las siguientes medidas:

    (a) El país donde se encuentra el receptor tiene, como mínimo, los mismos estándares de protección que los otorgados por la LPDP y su Reglamento; o
    (b) Existe un acuerdo escrito entre el receptor y Telxius, mediante el cual el receptor asume las mismas obligaciones que asume Telxius bajo la LPDP y su Reglamento.

16. Cuando los datos personales son necesarios para la ejecución de una relación contractual, Telxius no tiene la obligación de obtener el consentimiento del titular para realizar el flujo transfronterizo, en línea con lo dispuesto por la LPDP.

---

[9] **LPDP**
"***Artículo 2.- Definiciones***
Para todos los efectos de la presente Ley, se entiende por:
[…]
10. Flujo Transfronterizo: *transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban."*

V. DERECHOS ARCO

17. Los Derechos ARCO refieren a los derechos de Acceso, de Rectificación, de Cancelación y de Oposición, entre otros; que pueden ejercer los titulares frente a la entidad que trata sus datos. Los Derechos ARCO son los siguientes:

    (a) Información: el derecho que tiene el titular a ser informado de cuándo y por qué se tratan sus datos personales.

    (b) Acceso: el derecho que tiene el titular a obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos, la forma en la que sus datos fueron recopilados, las razones para ello, a solicitud de quien se realizó la recopilación, las transferencias realizadas, las condiciones de tratamiento, y el tiempo de conservación.

    (c) Rectificación: el derecho que tiene el titular a que se modifiquen o actualicen aquellos datos personales que resulten parcial o totalmente inexactos, incompletos, erróneos o falsos.

    (d) Cancelación: el derecho que tiene el titular a solicitar la supresión o cancelación de datos en un banco cuando: (i) estos hayan dejado de ser necesarios para las finalidades para la cual fueron recopilados; (ii) hubiera vencido el plazo para su tratamiento; (iii) decida revocar su consentimiento; y, (iv) no estén siendo tratados conforme a Ley.

        El ejercicio de este derecho no procede cuando los datos sean conservados en virtud de razones históricas, estadísticas o científica; cuando sean necesarios para el desarrollo y cumplimiento de una relación contractual; cuando deban ser tratados en virtud de una Ley, entre otros casos previstos en la normativa sobre la materia.

    (e) Revocación: el que tiene el titular a retirar el consentimiento para todas o ciertas finalidades del tratamiento de los datos.

    (f) Oposición: el derecho que tiene el titular a oponerse a determinadas formas de tratamiento que se dan a los datos personales en los siguientes supuestos: (i) cuando no hubiere prestado consentimiento para su recopilación por haber sido tomados de fuente de acceso al público; (ii) cuando habiendo prestado consentimiento, se acredita la existencia de motivos fundados y legítimos relativos a una concreta situación personal que genere un perjuicio al titular.

        El ejercicio de este derecho no procede en aquellos casos en los que el tratamiento de la información personal sea necesario para el cumplimiento de un mandato legal.

18. Telxius cuenta con las plataformas adecuadas para que los titulares de los datos personales puedan plantear solicitudes para ejercer sus Derechos ARCO.

Se han implementado dos canales de atención, según se informa en las Cláusulas Informativas y Cláusulas de Usos Adicionales de Telxius:

(i) Por escrito: el titular puede ejercer sus Derechos ARCO dirigiéndose a la sede administrativa de TELXIUS, ubicada en Avenida Paseo de la República No. 5895 (Edificio Leuro), Oficina 903, Lima, Perú, en el horario establecido; o

(ii) Por correo electrónico: el titular puede ejercer sus Derechos ARCO enviando su solicitud a la siguiente dirección electrónica: dpo.telxius@telxius.com.

El titular puede utilizar el documento "Solicitud para ejercicio de Derechos ARCO", que se encuentra en nuestras oficinas, el cual también podrá ser solicitado al correo consignado.

Para ello, el usuario debe cumplir con los requisitos mínimos establecidos en dicha solicitud, dependiendo del Derecho ARCO del que se trate. Sin perjuicio de ello, siempre debe adjuntar su documento de identidad; o, en caso la solicitud sea presentada por un representante, adicionalmente adjuntar copia de su documento de identidad y carta poder con firma legalizada.

19. El encargado frente a las solicitudes de ejercicio de Derechos ARCO que puedan ser presentadas es el Gerente General, el señor José Luis Díaz Ramírez, quien atiende las solicitudes presentadas en cumplimiento de los siguientes plazos:

- Derecho de Información: 8 días hábiles.
- Derecho de Acceso: 20 días hábiles.
- Derecho de Rectificación, Cancelación y/o Oposición: 10 días hábiles.
- Derecho de Revocación: 5 días hábiles.

Salvo en el caso del derecho de información, el plazo para la respuesta o atención podrá ser ampliado una sola vez y por un plazo igual, siempre y cuando las circunstancias lo justifiquen.

La respuesta será enviada a través de la vía de respuesta seleccionada por el usuario, sea mediante: (i) visualización en sitio; (ii) escrito, copia, fotocopia o facsímil; (iii) transmisión electrónica (correo); o, (iv) cualquier otra forma idónea.

VI. ADOPCIÓN DE MEDIDAS DE SEGURIDAD

20. Telxius tiene la obligación de adoptar medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales que trata.

21. Telxius cuenta con medidas apropiadas acordes con el tratamiento y categoría de datos personales que trata. Concretamente, Telxius adopta las siguientes medidas:

Para el caso de tratamiento automatizado:

- Sistema de control de acceso a la información, que incluye la gestión de accesos desde el registro de usuario, la gestión de los privilegios del usuario y su identificación ante el sistema.

  Ello se realiza a través de un sistema de usuarios y contraseñas, y de un registro de usuarios con acceso que se mantiene siempre actualizado.

- Revisión semestral de los privilegios asignados. El registro de la revisión periódica de privilegios se mantiene siempre actualizado.

- Generación y mantenimiento de registros que proveen evidencia sobre las interacciones con datos lógicos, incluyendo, para los fines de la trazabilidad, la información de cuentas de usuario con acceso al sistema, y horas de inicio y cierre de sesión. Estos registros cuentan con un procedimiento de disposición consistente en su borrado automático a los dos años.

- Mecanismo de respaldo de seguridad de la información de la base de datos personales con un procedimiento que contempla la verificación de los datos almacenados en el respaldo, incluyendo la recuperación completa ante una interrupción o daño, garantizando el retorno al estado en el que se encontraba al momento en que se produjo la interrupción o daño.

- Para la transferencia lógica o electrónica de datos personales, se cuenta con medidas de seguridad, tales como comunicaciones securizadas mediante cifrado, antimalware, antispam y SPF, destinadas a evitar el acceso no autorizado, pérdida o corrupción durante el tránsito de la información hacia su destino.

Para el caso de tratamiento no automatizado:

Los armarios y archivadores en los que se almacenan los documentos se encuentran en áreas en las que el acceso está protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente a los que solo tiene acceso el personal autorizado. Cada persona autorizada cuenta con solo una llave o dispositivo de acceso. Estas áreas permanecen cerradas y solo debe acceder el personal autorizado.

- Generación y mantenimiento de registros que proveen evidencia sobre el acceso del personal que ha tenido acceso a los datos personales.

- Para el traslado de información no automatizada, se adoptan las medidas para impedir el acceso o manipulación de la información, tales como el uso de contenedores que evitan su acceso y legibilidad.

- Cuando la información es destruida, se mantiene un control de inventario en el que se señala qué información fue eliminada.

Para el caso de tratamiento automatizado y no automatizado:

- La generación de copias o reproducción de la información únicamente se realiza por el personal autorizado para ello. Los equipos de reproducción (por ejemplo, máquinas de fotocopiado, escaners, hasta puertos USB o unidades de grabación digital en ordenadores personales), cuentan con claves, se supervisa el uso de los equipos y se retiran los documentos originales y las copias inmediatamente. Estas se destruyen antes de ser desechadas.

- El acceso del personal a datos personales se encuentra limitado estrictamente a los supuestos en los que es necesario su tratamiento.

- Telxius cuenta con cláusulas con terceros y encargados en donde se recoge expresamente la prohibición de acceder a los datos personales con fines distintos a los estipulados y la obligación de secreto respecto a los datos que hubiera podido conocer con motivo de la prestación.

22. El responsable de la seguridad de los bancos de datos personales es el Gerente General, el señor José Luis Díaz Ramirez.

23. Adicionalmente, Telxius revisa periódicamente la efectividad de las medidas de seguridad adoptadas y su conocimiento por parte de sus colaboradores.

24. Sin perjuicio de lo señalado, cabe añadir que Telxius asegura el cumplimiento del deber de confidencialidad haciendo que sus Trabajadores, Practicantes, Clientes, Proveedores y Terceros y Encargados firmen una cláusula de confidencialidad.

VII. OBLIGACIONES EN MATERIA DE VIDEOVIGILANCIA

25. El tratamiento a través de sistemas de videovigilancia comprende tanto la grabación, captación, transmisión, conservación o almacenamiento de imágenes o voces e incluye la reproducción o emisión en tiempo real de datos personales para fines de seguridad, control laboral, entre otros.

26. Telxius mantiene sistemas de videovigilancia para el control de accesos a sus instalaciones (zonas comunes, periferia y de tránsito).

27. En ese sentido, al constituir el uso de sistemas de videovigilancia un supuesto de tratamiento de datos personales, para cumplir con el deber de informar, la zona videovigilada debe tener un cartel o anuncio visible con fondo amarillo o cualquier otro que contraste con el color de la pared y ser lo suficientemente visible.

    Por ello, Telxius cuenta en cada acceso a zona videovigilada con un cartel informativo que indica:

    (i) La identidad y domicilio de Telxius como titular del banco de datos;
    (ii) Ante quién y cómo se pueden ejercitar los Derechos ARCO.
    (iii) Lugar dónde puede obtener la información contenida en el artículo 18 de la LPDP.

    Estos carteles tienen las dimensiones de 297 x 210 mm y se basan en el siguiente modelo, aprobado por la Autoridad de Datos:

28. Además, Telxius cuenta con una Cláusula Informativa de Videovigilancia, disponible de forma impresa en las oficinas y/o locales de Telxius donde se cuente con un sistema de videovigilancia, que cumple con informar lo siguiente:

    - La identidad y domicilio del titular del banco de datos personales y del encargado del tratamiento, de ser el caso.
    - La finalidad.
    - Las transferencias y destinatarios de los datos personales.
    - El plazo durante el cual se conservarán los datos personales.
    - El ejercicio de los derechos de información, acceso, cancelación y oposición de los datos.

29. Cabe precisar que Telxius no se encuentra obligado a solicitar el consentimiento para la transferencia de los datos personales captados por los sistemas de videovigilancia cuando (i) lo captado deba ser entregada por orden judicial o (ii) cuando deba ser puesto a disposición o sea requerido por la Policía Nacional del Perú o el Ministerio Público.

30. Dadas las particularidades de los sistemas de videovigilancia, los usuarios pueden ejercer cualquiera de sus Derechos ARCO, salvo el Derecho de Rectificación, toda vez que las imágenes captadas reflejan un hecho objetivo que no puede ser modificado.

31. Telxius almacena por un plazo de treinta (30) días hábiles las imágenes captadas mediante el sistema de videovigilancia. Las imágenes se borran dentro de los dos (2) días hábiles de vencido este plazo.

32. Telxius asegura la reserva y confidencialidad de la información, no permitiendo la difusión, copia o visualización de imágenes por parte de terceros no autorizados. Para ello, cumple con:

    - Tener un procedimiento de identificación y autentificación de usuarios que den cuenta del funcionamiento del sistema de videovigilancia;
    - Conocer el funcionamiento correcto del sistema de videovigilancia;
    - Contar con un inventario documentado de las cámaras;
    - Contar con un esquema documentado de la arquitectura física y lógica del sistema de videovigilancia;
    - Contar con documentación respecto a la gestión de accesos, privilegios y verificación periódica de privilegios asignados;
    - Contar con mecanismos de respaldo de seguridad de la información, así como con un procedimiento que contempla la verificación de la integridad de los datos almacenados en el respaldo;
    - Contar con medidas de seguridad en caso sea necesario transportar los sistemas que contengan información de carácter personal
    - Otras obligaciones regulatorias.

    El acceso únicamente lo tiene el usuario con perfil de administrador, el señor Ronald Chávez, quien ha firmado una cláusula de confidencialidad en su contrato de trabajo.

33. Telxius no tiene instaladas cámaras de seguridad en baños ni vestuarios, y no graba las conversaciones de personas ni utiliza las imágenes captadas con fines comerciales o promocionales.

*****