Política Corporativa de Protección de Datos

Consejero Delegado
29/10/2024

CONTROL DE VERSIONES

Versión	Fecha	Cambios
V1	03/03/2023	Nueva Creación
V2	29/10/2024	Actualización de contenido

CONTENIDO

1. Objeto

La finalidad de esta Política Corporativa de Protección de Datos (en adelante, la "Política") es establecer los principios y pautas comunes y generales de actuación que deben regir en materia de protección de datos personales para todas las empresas que componen el Grupo Urbaser u otras comprendidas en el Ámbito de aplicación, con el fin de promover, en todo caso, el cumplimiento de la legislación aplicable.

En particular, la Política garantiza el derecho a la protección de los datos de todas las personas físicas que se relacionan con las sociedades del Ámbito de aplicación, asegurando el respeto del derecho al honor, a la privacidad y a la intimidad en el tratamiento de las diferentes tipologías de datos personales, procedentes de diferentes fuentes y con fines diversos en función de la actividad empresarial que se desarrolle.

2. Ámbito de Aplicación

Este documento es de obligada aplicación en la totalidad de las entidades participadas (Sociedades, UTEs, Joint Ventures y otras asociaciones equivalentes) en las que URBASER, S.A.U. sea el socio mayoritario o tenga el control, y de obligado cumplimiento a todo usuario que participe en la gestión, uso o explotación de los datos personales que se generen y traten en URBASER, incluido, pero no limitado a consejeros/as, directivos/as, empleados/as, colaboradores, gerentes, miembros de los órganos de gobiernos, todo ello sin perjuicio de la legislación y requerimientos legales específicos que resulten de aplicación en cada país

En aquellas entidades participadas en las que esta Política no sea de aplicación, se promoverá, a través de sus representantes en los órganos de administración, el alineamiento de sus políticas propias con las de la presente Política.

IMPORTANTE: En caso de existir normativa local o sectorial que contravenga lo establecido en la presente política, cada país o región deberá adecuarlo a la legislación que resulte aplicable. Todo ello teniendo en cuenta que este documento contempla unas garantías mínimas en materia de protección de datos que deberán ser respetadas en todo momento, y que no podrán ser modificadas para hacerlas menos eficaces.

3. Contenido

- **Principios y consideraciones generales relativas al tratamiento de datos personales.**

Se cumplirá estrictamente con la legislación aplicable en materia de protección de datos, en función del tratamiento de datos personales que se lleve a cabo y lo que se determine conforme a normas o procedimientos adoptados en el seno del Grupo.

Asimismo, se promoverá que los principios y consideraciones recogidas en la presente Política sean tenidas en cuenta: (i) en el diseño e implementación de procedimientos que impliquen un tratamiento de datos personales; (ii) en los productos y servicios ofrecidos; (iii) en la contratación de servicios que conlleve un tratamiento de datos personalesy; (iv) en la implantación de cuantos sistemas y plataformas permitan el acceso por parte de los profesionales del Grupo o de terceros a datos personales y a la recogida o tratamiento de dichos datos.

Conforme a lo anterior, cualquier tratamiento de datos personales que se realice en el Grupo, deberá observar los siguientes principios y consideraciones generales:

a) Principios de legitimidad, licitud y lealtad en el tratamiento de datos personales

El tratamiento de datos personales será legítimo, lícito y leal. En este sentido, únicamente se podrá llevar a cabo un tratamiento de datos personales cuando exista una base legal que lo habilite, como el consentimiento del interesado, el contrato de trabajo, el cumplimiento de obligaciones legales, el interés público o los intereses legítimos perseguidos por el Responsable del tratamiento, siempre respetando los derechos y libertades de los interesados.

Esta habilitación legal debe ser documentada, garantizando su disponibilidad para su revisión y auditoría.

Asimismo, los datos personales deberán ser tratados de manera justa y leal, lo que implica que la entidad no los puede utilizar

de manera engañosa o fraudulenta.

No se recabarán ni tratarán datos personales relativos al origen étnico o racial, a la ideología política, a las creencias, a las convicciones religiosas o filosóficas, a la vida u orientación sexual, a la afiliación sindical, a la salud, ni datos genéticos o biométricos dirigidos a identificar de manera unívoca a una persona, salvo que exista una habilitación legal conforme a la normativa de protección de datos y/o normativa local que resulte de aplicación, en cuyo caso, se deberá acreditar que el tratamiento es necesario, legítimo y proporcional, no existiendo métodos alternativos con los que se pueda satisfacer la misma finalidad.

b) Principio de minimización

Solo serán objeto de tratamiento aquellos datos personales que resulten estrictamente necesarios para la finalidad para la que se recojan, es decir, serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que sean tratados.

c) Principio de exactitud

Los datos personales deberán ser exactos y estar actualizados, adoptándose medidas razonables para que el interesado pueda solicitar su rectificación o supresión cuando en cada caso corresponda.

d) Principio de limitación de la finalidad y del plazo de conservación

Los datos personales se recabarán para fines determinados, explícitos y legítimos y no se tratarán ulteriormente de manera incompatible.

El tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales, siempre y cuando se tengan en cuenta el resto de los principios.

Asimismo, los datos personales no se conservarán más allá del plazo necesario para conseguir el fin para el cual fueron recabados, salvo en los supuestos previstos legalmente.

e) Principios de integridad y confidencialidad

En el tratamiento de los datos personales se deberá garantizar, mediante medidas técnicas y organizativas, una seguridad adecuada que los proteja del tratamiento no autorizado o ilícito y que evite su pérdida, destrucción y/o daño accidental.

Los datos personales recabados y tratados por las entidades del Grupo deberán ser conservados con la máxima confidencialidad y secreto, no pudiendo ser utilizados para otros fines distintos de los que justificaron y permitieron su recogida, sin que puedan ser comunicados o cedidos a terceros fuera de los casos permitidos por la legislación aplicable.

f) Principio de responsabilidad proactiva (rendición de cuentas)

Las entidades del Grupo serán responsables de cumplir con los principios estipulados en esta Política y los exigidos en la legislación aplicable y deberán ser capaces de demostrarlo.

Para ello, se evaluarán de forma previa los riesgos que para la protección de datos personales puedan comportar nuevos tratamientos, productos, servicios o sistemas de información y se adoptarán las medidas necesarias para eliminarlos o mitigarlos. En los casos en los que la ley lo requiera, deberán realizar una evaluación del riesgo de aquellos tratamientos que entrañen un riesgo elevado para los derechos y libertades de los interesados, con el fin de determinar las medidas a aplicar para garantizar que los datos personales se tratan conforme a las exigencias legales.

Asimismo, se deberá llevar a cabo un registro o inventario de actividades en el que se describan los tratamientos de datos personales que lleven a cabo en el marco de sus actividades.

En los casos previstos en la ley, se designará a delegados de protección de datos (“DPD”), con el fin de garantizar el cumplimiento de la normativa de protección de datos en las entidades del Grupo. En ausencia de DPD, se podrán designar Coordinadores de Protección de Datos.

g) Principios de transparencia e información

El tratamiento de datos personales será transparente en relación con la persona interesada, facilitándole la información sobre el tratamiento de sus datos de forma comprensible y accesible.

A fin de garantizar un tratamiento leal y transparente, la entidad del Grupo responsable del tratamiento deberá informar a las personas afectadas o interesadas cuyos datos se pretende recabar, en concreto:

- la identidad y los datos de contacto del Responsable del tratamiento;

- el fin del tratamiento de los datos;
- los terceros o categorías de terceros a los que se transfieren en su caso los datos;
- la base jurídica del tratamiento;
- los derechos de protección de datos que pueden ser ejercitados por los interesados.
- la intención de realizar transferencias internacionales, si fuera el caso;
- el plazo de conservación de los datos;
- los datos de contacto del Delegado de Protección de Datos, si fuera el caso.

h) Adquisición u obtención de datos personales

Queda prohibida la adquisición u obtención de datos personales de fuentes ilegítimas, de fuentes que no garanticen suficientemente su legítima procedencia o de fuentes cuyos datos hayan sido recabados o cedidos contraviniendo la ley.

i) Contratación de encargados de tratamiento

Con carácter previo a la contratación de cualquier prestador de servicios que acceda a datos personales que sean responsabilidad de las entidades del Grupo, así como durante la vigencia de la relación contractual, se deberán adoptar las medidas necesarias para garantizar que ofrece un nivel de seguridad adecuado.

Asimismo, una vez se verifique un nivel de seguridad adecuado del proveedor de servicios que van a tener acceso a los sistemas de información de cualesquiera de las empresas que componen el Grupo, se suscribirán los correspondientes contratos de encargo de tratamiento de datos personales, en aquellos casos en los que resulte de aplicación.

j) Transferencias internacionales de datos

Cuando un tratamiento conlleve una transferencia internacional de datos personales a un tercer país u organización internacional que no ofrezca el mismo nivel de garantías, se deberán adoptar las medidas necesarias con el objeto de reforzar la seguridad de los datos personales, de manera que únicamente se podrá llevar a cabo mediante el establecimiento de garantías adecuadas.

Asimismo, las entidades del Grupo ubicadas fuera del Espacio Económico Europeo, deberán cumplir con los requisitos establecidos para las transferencias internacionales de datos personales que sean, en su caso, de aplicación en su jurisdicción.

k) Derechos de las personas interesadas

Las entidades del Grupo deberán permitir que las personas interesadas puedan ejercitar los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición que sean de aplicación en cada jurisdicción, estableciendo, a tal efecto, los procedimientos internos que resulten necesarios.

l) Brechas de seguridad

En el caso de que se produzca un incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizado a dichos datos, se deberá seguir la Política Corporativa de Seguridad de la Información del Grupo, así como los procedimientos internos que la desarrollan. Dichos incidentes deberán documentarse y se adoptarán medidas para solventar y mitigar los posibles efectos negativos para los interesados.

m) Registro de Actividades del Tratamiento

Se deberá llevar a cabo un registro o inventario en donde se describan todas las actividades desarrolladas en la organización que conlleven un tratamiento de datos personales.

De esta forma, todas las empresas del Grupo deberán mantener un inventario que incluya, como mínimo, el conjunto de actividades de tratamiento, finalidades y su correspondiente descripción, tipología de datos tratados, y otra serie de cuestiones relacionadas con el tratamiento de datos personales llevado a cabo por el responsable.

4. Implementación

Con el objeto de garantizar el cumplimiento de la presente Política, cada empresa del Grupo dedicará los recursos adecuados

para su implementación, mantenimiento y revisión, y desarrollarán los procedimientos internos de carácter local que sean necesarios para materializar su contenido, adecuándolo a las novedades normativas que se produzcan, siempre de forma alineada con la política y procedimientos corporativos.

5. Formación

Se promoverán las medidas de formación y concienciación necesarias para el conocimiento y la cultura en materia de protección de datos, que se deberán impartir, de manera periódica, para el aumento de los conocimientos de los empleados, en particular, de aquellos que tengan acceso a los sistemas de información.

6. Control y supervisión

El Delegado de Protección de Datos supervisará el cumplimiento de lo dispuesto en esta Política, de manera conjunta con los distintos Coordinadores de Protección de Datos designados a nivel nacional e internacional, que serán los encargados de establecer e implementar procedimientos internos de carácter local, adaptando su contenido en función de la ley aplicable en sus respectivas jurisdicciones.

7. Dudas, comunicaciones o denuncias

Las consultas en el ámbito de esta Política deben ser dirigidas al Departamento Corporativo de Ciberseguridad y de Protección de Datos de URBASER a la dirección habilitada: pdp@urbaser.com.

Cualquier incidencia en relación con el incumplimiento de lo establecido en esta Política y procedimientos relacionados, o su alineamiento con lo establecido en el Código de Conducta del Grupo, deberá dirigirse al órgano de cumplimiento normativo correspondiente a través del Canal Ético habilitado en la página web del Grupo (www.urbaser.com).

8. Incumplimientos

La presente Política tiene la consideración de una norma de obligado cumplimiento, por lo que su vulneración supondrá una infracción de esta y la Compañía adoptará las medidas disciplinarias, contractuales o legales que sean procedentes, en su caso, sin perjuicio de otras responsabilidades en que el infractor hubiera podido incurrir. Igualmente, URBASER se reservará el derecho de adoptar las medidas que considere oportunas contra los socios comerciales que la incumplan. Cualquier excepción o exención, ya sea por motivos organizativos, legales, contractuales, tecnológicos o de otra índole a esta Política o a cualquier norma, procedimiento o instrucción técnica del que dependa, será gestionada conforme a los documentos internos definidos para ello.

9. Revisión y actualización

El Departamento Corporativo de Ciberseguridad y Protección de Datos, revisará periódicamente el contenido de esta Política Corporativa, asegurándose de que recoge las recomendaciones y mejores prácticas en vigor y propondrá al Comité de Seguridad de la Información, las modificaciones y actualizaciones que contribuyan a su desarrollo, aprobación y mejora continua.

www.urbaser.com