



Política Corporativa de Protección de Datos

Consejero Delegado
3 marzo 2023

CONTROL DE VERSIONES

Versión	Fecha	Cambios
V1	03/03/2023	Nueva Creación

CONTENIDO

1. Objeto	4
2. Ámbito de Aplicación	4
3. Contenido	4
4. Formación	6
5. Dudas, comunicaciones o denuncias	6
6. Incumplimientos	6
7. Revisión y actualización	7

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 dicha materia.

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

Esta Política es de 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 (en adelante “el Grupo”).

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.

3. Contenido

Principios generales relativos 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 proceda llevar a cabo conforme a la finalidad pretendida.

Asimismo, se promoverá que los principios recogidos en esta Política sean tenidos en cuenta: (i) en el diseño e implementación de todos los procedimientos que impliquen el tratamiento de datos personales; (ii) en los productos y servicios ofrecidos; (iii) en la contratación con tratamiento de datos personales; y (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.

Principios básicos relativos al tratamiento de datos personales

Los principios relativos al tratamiento de los datos personales sobre los que se fundamenta esta Política son los que se detallan a continuación:

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

El tratamiento de datos personales será legítimo, lícito y leal, conforme a la legislación aplicable. En este sentido, los datos personales deberán ser recogidos para uno o varios fines específicos y legítimos conforme a la legislación aplicable.

En los casos en los que resulte obligatorio, conforme a la legislación aplicable, deberá obtenerse el consentimiento de los interesados antes de recabar sus datos.

Asimismo, cuando lo exija la Ley, los fines del tratamiento de datos personales serán explícitos y determinados en el momento de su recogida.

En particular, 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 la recogida de los referidos datos sea necesaria, legítima y requerida o permitida por la legislación aplicable, en cuyo caso serán recabados y tratados de acuerdo con lo establecido en aquella.

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. En caso contrario, deberán suprimirse o rectificarse.

d) Principio de limitación del plazo de conservación.

Los datos personales no se conservarán más allá del plazo necesario para conseguir el fin para el cual se tratan, 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 asimismo 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, cuando así lo exija la Ley. Para ello, 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. En los casos en los que la ley lo requiera, se evaluarán de forma previa los riesgos que para la protección de datos personales puedan comportar nuevos productos, servicios o sistemas de información y se adoptarán las medidas necesarias para eliminarlos o mitigarlos.

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

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, deberán seguirse los protocolos internos establecidos a tal efecto por la Política Corporativa de Seguridad de la Información del Grupo, y por los que establezca la legislación aplicable. Dichos incidentes deberán documentarse y se adoptarán medidas para solventar y paliar los posibles efectos negativos para los interesados.

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 podrá designar a coordinadores en 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, cuando así lo exija la ley aplicable.

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, de las circunstancias relativas al tratamiento conforme a la legislación aplicable.

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 y, cuando sea legalmente exigible, demostrar, que el tratamiento de datos por parte del encargado de tratamiento se lleva a cabo conforme a la normativa aplicable.

j) Transferencias internacionales de datos.

Todo tratamiento de datos personales sujeto a la normativa de la Unión Europea que implique una transferencia de datos fuera del Espacio Económico Europeo deberá llevarse a cabo con estricto cumplimiento de los requisitos establecidos en la ley aplicable en la jurisdicción de origen. Asimismo, las entidades del Grupo ubicadas fuera de la Unión Europea 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 para satisfacer, al menos, los requisitos legales aplicables en cada caso.

4. Implementación

Las entidades del Grupo, en función de la ley aplicable en sus respectivas jurisdicciones, establecerán procedimientos internos de carácter local que desarrollen los principios recogidos en esta Política y que materialicen su contenido y lo adecúen a las novedades normativas que se produzcan en el ámbito de la protección de datos personales.

Las Direcciones Corporativas de Tecnologías de la Información y Ciberseguridad del Grupo, serán las encargadas de implementar en los sistemas de información de las entidades del Grupo, los controles y desarrollos informáticos que sean adecuados para garantizar el cumplimiento de la normativa interna de la protección de datos y velarán por que dichos desarrollos estén actualizados en cada momento.

5. Formación

Se promoverán complementariamente las medidas de formación necesarias para el conocimiento, implantación y seguimiento de la presente Política en materia de protección de datos personales.

5. Dudas, comunicaciones o denuncias

Las consultas en el ámbito de esta Política deben ser dirigidas al Área Corporativa de Protección de Datos de URBASER, S.A.U, por medio escrito 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).

6. Incumplimientos

La presente Política tiene la consideración de norma de obligado cumplimiento, por lo que su vulneración supondrá una infracción y se adoptarán las medidas disciplinarias que resulten procedentes, en su caso, sin perjuicio de otras responsabilidades en que el infractor hubiera podido incurrir. Igualmente, URBASER, S.A.U. se reservará el derecho de adoptar las medidas que considere oportunas contra los socios comerciales que la incumplan.

7. Revisión y actualización

El Área Corporativa de Protección de Datos, dependiente del Departamento Corporativo de Asesoría Jurídica, revisará periódicamente el contenido de esta Política Corporativa, asegurándose de que recoge las recomendaciones y mejores prácticas en vigor, y propondrá al órgano de administración las modificaciones y actualizaciones que contribuyan a su desarrollo y mejora continua.



www.urbaser.com