Corporate Data Protection Policy

CEO
3rd March 2023

VERSION CONTROL

Version	Date	Changes
V1	03/03/2023	New Document

CONTENTS

1. Purpose

The purpose of this Corporate Policy (hereinafter, the "Policy") is to establish the common and general principles and guidelines for action that shall govern the protection of personal data for all entities that comprise Grupo Urbaser and any others that are within its Scope of application, in order to promote, at all times, compliance with applicable law.

In particular, the Policy guarantees the right to data protection of all natural persons who are related to the entities within the Scope of application, ensuring respect for the right to honour, privacy and intimacy in the processing of different types of personal data from a variety of sources and for several purposes, depending on the business activity being carried out.

2. Scope of application

This Policy applies to all the investees (Companies, UTEs, Joint Ventures and other equivalent associations) to which URBASER, S.A.U. is the majority shareholder or has control of (hereinafter "the Group").

For those investees to which this Policy is not applicable, the alignment of their own policies with those of the investee shall be promoted through their representatives in the management bodies.

3. Content

General principles governing the processing of personal data.

Applicable data protection legislation will be scrupulously enforced, depending on the processing of personal data to be carried out and its intended purpose.

Likewise, the principles set forth in this Policy shall be considered: (i) in the design and implementation of all procedures involving the processing of personal data; (ii) in the products and services offered; (iii) in any contracts entailing the processing of personal data; and (iv) in the implementation of all systems and platforms that allow access by the Group professionals or third parties to personal data and the collection or processing of such data.

Basic principles governing the processing of personal data.

The principles upon which this Policy is founded are detailed below:

a) Principle of lawfulness, fairness, and transparency

The processing of personal data shall be legitimate, lawful, and fair in accordance with the applicable legislation. In this sense, personal data shall be collected for one or more specific and legitimate purposes in accordance with the applicable legislation.

When required by applicable law, the consent of the data subjects shall be obtained prior to the collection of their data.

Likewise, when required by law, the purposes of processing shall be explicit and determined at the time of collection.

In particular, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual life or sexual orientation, health, or genetic or biometric data aimed at univocally identifying a natural person shall not be processed, unless the processing of such data is necessary, legitimate and required or permitted by the applicable legislation, in which case they shall be collected and processed in accordance with the provisions of that legislation.

b) Principle of data minimisation

Only personal data that are strictly necessary for the purpose for which they are collected, i.e., adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed, shall be processed.

c) Principle of accuracy

Personal data must be accurate and up to date. Otherwise, they must be deleted or corrected.

d) Principle of storage limitation

Personal data will not be kept for longer than is necessary to achieve the purpose for which they are processed, except in the cases provided for by law.

e) Principles of integrity and confidentiality

The processing of personal data shall ensure, by means of technical and organisational measures, adequate security to protect them from unauthorised or unlawful processing and to prevent their accidental loss, destruction and/or damage.

Personal data processed by the Group entities must be kept with the utmost confidentiality and secrecy and shall not be used for purposes other than those that motivated and authorised their collection, nor communicated or transferred to third parties outside the cases permitted by the applicable legislation.

f) Principle of accountability

Group entities shall be responsible for complying with the principles set forth in this Policy and those required by applicable law and shall be able to demonstrate such compliance, when required by law. To this end, they shall conduct a risk assessment on processing operations that entail a high risk to the rights and freedoms of the data subjects, in order to determine the measures to be applied to ensure that personal data are processed in accordance with legal requirements. Where required by law, the risks that new products, services, or information systems may entail for the protection of personal data shall be assessed in advance, and the necessary measures shall be adopted to eliminate or mitigate them.

Likewise, Group entities shall keep an activity log describing the processing of personal data performed in the course of their activities.

Should an incident occur that results in the accidental or unlawful destruction, loss or alteration of personal data, or unauthorised communication or access to such data, the internal protocols established for this purpose by the Group's Corporate Information Security Policy, and those established by the applicable legislation, must be followed. Such incidents shall be documented, and measures shall be adopted to solve and mitigate the possible negative effects on the data subjects.

In the cases provided for by law, a Data Protection Officer ("DPO") shall be appointed to ensure compliance with data protection regulations in the Group entities. In the absence of a DPO, a data coordinator can be appointed.

g) Transparency and information principles

The processing of personal data shall be transparent in relation to the data subject, providing them with the information on the processing of their data in an understandable and accessible manner, where required by applicable law.

In order to ensure fair and transparent processing, the Group entity responsible for the processing shall inform the data subjects whose data is intended to be collected of the circumstances relating to the processing in accordance with the applicable law.

h) Acquisition or collection of personal data

It is prohibited to acquire or obtain personal data from illegitimate sources, from sources that do not provide sufficient guarantee of their legitimate origin or from sources whose data have been collected or transferred in breach of the law.

i) Data processors

Prior to contracting any service provider that accesses personal data under the responsibility of the Group entities, and over the term of the contractual relationship, the necessary measures shall be adopted to guarantee and, when legally required, to demonstrate that the processing by the data processor is carried out in accordance with the applicable regulations.

j) International transfers of personal data

Any processing of personal data subject to European Union regulations that entail a transfer of data outside the European Economic Area shall be carried out in strict compliance with the requirements established in the applicable law of the jurisdiction of origin. Likewise, Group entities outside the European Union shall comply with the requirements established for international transfers of personal data that are, where applicable, enforceable in their home country's jurisdiction.

k) Rights of the data subject

The Group entities shall allow data subjects to exercise the rights of access, rectification, erasure, restriction of processing, portability, and objection, applicable in each jurisdiction, establishing to this effect, the necessary internal procedures to satisfy, at least, the legal requirements in each case.

4. Implementation

The Group entities, pursuant to the law applicable in their respective jurisdictions, shall establish internal procedures of domestic nature that further develop the principles set forth in this Policy and that materialise its content and adapt it to the regulatory developments that may take place in connection with the protection of personal data.

The Group's Corporate Information Technology and Cybersecurity Departments shall be responsible for implementing the appropriate IT controls and developments in the information systems of the Group entities to ensure compliance with internal data protection regulations and that such developments are up to date at all times.

5. Training

Training initiatives shall be promoted for the acknowledgement, implementation, and monitoring of this Policy on personal data protection.

6. Doubts, communications, or complaints

Queries related to data protection shall be addressed to the URBASER, S.A.U. Corporate Data Protection Area, by written means to the following address: pdp@urbaser.com.

Any incident regarding non-compliance with the provisions of this Policy and related procedures, or its alignment with the provisions of the Group's Code of Conduct, shall be addressed to the corresponding regulatory compliance body through the Ethics Channel accessible on the Group website (www.urbaser.com).

7. Non-compliance

Compliance with this Policy is mandatory. Therefore, its violation will constitute an infringement and, where appropriate, the corresponding disciplinary measures will be applied, without prejudice to any other responsibilities that the infringer may have incurred. Likewise, URBASER, S.A.U. reserves the right to adopt the measures it deems appropriate against business partners who fail to comply with it.

8. Review and updating

The Corporate Data Protection Area, which reports to the Corporate Legal Department, will periodically review the content of this Corporate Policy, ensuring that it reflects the recommendations and best practices in force, and will propose to the management body the modifications and updates that contribute to its development and continuous improvement.

www.urbaser.com