Corporate Data Protection Policy

Chief Executive Officer
29/10/2024

VERSION CONTROL

Version	Date	Changes
V1	03/03/2023	New creation
V2	29/10/2024	Content update

CONTENTS

1. Object

The purpose of this Corporate Data Protection Policy (hereinafter, the "Policy") is to establish the common and general principles and guidelines for action that must govern the protection of personal data for all the companies that make up the Urbaser Group or others included in the Scope of application, in order to promote, in all cases, compliance with the applicable legislation.

In particular, the Policy guarantees the right to data protection of all natural persons who come into contact with the companies in the Scope of application, ensuring respect for the right to honour, privacy and intimacy in the processing of different types of personal data, from different sources and for different purposes depending on the business activity being carried out.

2. Scope of application

This document must be applied to all the investee entities (Companies, UTEs, Joint Ventures and other equivalent associations) in which URBASER, S.A.U. is the majority shareholder or has control. is the majority shareholder or has control, and of obligatory compliance for all users who participate in the management, use or exploitation of the personal data generated and processed in URBASER, including, but not limited to directors, managers, employees, collaborators, managers, members of the governing bodies, all without prejudice to the specific legislation and legal requirements that may be applicable in each country.

In those investee entities in which this Policy does not apply, the alignment of their own policies with those of this Policy will be promoted through their representatives in the governing bodies.

IMPORTANT: In the event of local or sectorial regulations that contravene the provisions of this policy, each country or region must adapt it to the applicable legislation. All of this taking into account that this document contemplates minimum data protection guarantees that must be respected at all times, and that may not be modified to make them less effective.

3. Content

- **General principles and considerations relating to the processing of personal data.**

Applicable data protection legislation will be strictly complied with, depending on the processing of personal data and as determined in accordance with rules or procedures adopted within the Group.

Likewise, the principles and considerations contained in this Policy shall be taken into account: (i) in the design and implementation of procedures involving the processing of personal data; (ii) in the products and services offered; (iii) in the contracting of services involving the processing of personal data; and (iv) in the implementation of any systems and platforms that allow access by the Group's professionals or third parties to personal data and the collection or processing of such data.

In accordance with the foregoing, any processing of personal data carried out within the Group shall observe the following general principles and considerations:

a) Principles of legitimacy, lawfulness and fairness in the processing of personal data

The processing of personal data shall be lawful, lawful and fair. In this regard, personal data may only be processed when there is a legal basis for doing so, such as the consent of the data subject, the employment contract, compliance with legal obligations, the public interest or the legitimate interests pursued by the Data Controller, always respecting the rights and freedoms of data subjects.

This legal clearance must be documented, ensuring its availability for review and audit.

Personal data must also be processed fairly and fairly, which means that the entity may not use them in a misleading or fraudulent manner.

No personal data relating to racial or ethnic origin, political ideology, beliefs, religious or philosophical convictions, sexual life or orientation, trade union membership, health, or genetic or biometric data intended to uniquely identify an individual will be collected or processed, unless there is a legal authorisation in accordance with the applicable data protection and/or local

regulations, in which case, it must be demonstrated that the processing is necessary, legitimate and proportional, and that there are no alternative methods with which the same purpose can be satisfied.

b) Minimisation principle

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, will be processed.

c) Principle of accuracy

Personal data must be accurate and up to date and reasonable steps must be taken to enable the data subject to request its rectification or erasure where appropriate.

d) Principle of purpose limitation and limitation of storage period

Personal data shall be collected for specified, explicit and legitimate purposes and shall not be further processed in an incompatible manner.

Further processing of personal data for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes, provided that the other principles are taken into account.

Likewise, personal data will not be kept beyond the period necessary to achieve the purpose for which they were collected, except in the cases provided for by law.

e) Principles of integrity and confidentiality

In the processing of personal data, adequate security must be ensured by means of technical and organisational measures to protect them from unauthorised or unlawful processing and to prevent their accidental loss, destruction and/or damage.

The personal data collected and processed by the entities of the Group must be kept with the utmost confidentiality and secrecy, and may not be used for purposes other than those that justified and permitted their collection, and may not be communicated or transferred to third parties outside the cases permitted by the applicable legislation.

f) Principle of proactive responsibility (accountability)

Group entities shall be responsible for and shall be able to demonstrate compliance with the principles set out in this Policy and those required by applicable law.

To this end, the risks to the protection of personal data that new processing, products, services or information systems may entail shall be assessed in advance and the necessary measures shall be adopted to eliminate or mitigate them. Where required by law, they shall carry out a risk assessment of those processing operations that entail a high risk to the rights and freedoms of data subjects, in order to determine the measures to be applied to ensure that personal data are processed in accordance with legal requirements.

They must also keep a register or inventory of activities describing the processing of personal data carried out in the course of their activities.

In the cases provided for by law, Data Protection Officers ("DPOs") shall be appointed to ensure compliance with data protection regulations in the Group's entities. In the absence of DPOs, Data Protection Coordinators may be appointed.

g) Principles of transparency and information

The processing of personal data shall be transparent in relation to the data subject by providing him or her with information on the processing of his or her data in an understandable and accessible manner.

In order to ensure fair and transparent processing, the Group entity responsible for the processing must inform the data subjects or interested parties whose data it intends to collect, in particular:

- the identity and contact details of the Controller;
- the purpose of the data processing;
- the third parties or categories of third parties to whom the data may be transferred;
- the legal basis for the processing;
- the data protection rights that can be exercised by data subjects.

- the intention to make international transfers, if any;
- the data retention period;
- the contact details of the Data Protection Officer, if applicable.

h) Acquisition or collection of personal data

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

i) Recruitment of data processors

Prior to contracting any service provider that accesses personal data for which the Group entities are responsible, as well as during the term of the contractual relationship, the necessary measures must be taken to ensure that it offers an adequate level of security.

Likewise, once an adequate level of security of the service provider that will have access to the information systems of any of the companies comprising the Group has been verified, the corresponding personal data processing contracts shall be signed, in those cases in which it is applicable.

j) International data transfers

Where a processing operation involves an international transfer of personal data to a third country or international organisation which does not provide the same level of safeguards, the necessary measures must be taken in order to strengthen the security of personal data, so that it can only be carried out by establishing appropriate safeguards.

Likewise, the entities of the Group located outside the European Economic Area must comply with the requirements established for international transfers of personal data that may be applicable in their jurisdiction.

k) Rights of the persons concerned

Group entities shall enable data subjects to exercise the rights of access, rectification, erasure, restriction of processing, portability and objection applicable in each jurisdiction, establishing the necessary internal procedures for this purpose.

l) Security breaches

In the event of an incident resulting in the accidental or unlawful destruction, loss or alteration of personal data, or unauthorised communication or access to such data, the Group's Corporate Information Security Policy, as well as the internal procedures that implement it, must be followed. Such incidents shall be documented and measures shall be taken to resolve and mitigate the possible negative effects on the data subjects.

m) Record of Processing Activities

A record or inventory should be kept describing all activities carried out in the organisation that involve the processing of personal data.

In this way, all Group companies must keep an inventory that includes, as a minimum, the set of processing activities, purposes and their corresponding description, type of data processed, and other matters related to the processing of personal data carried out by the controller.

4. Implementation

In order to ensure compliance with this Policy, each Group company will dedicate the appropriate resources to its implementation, maintenance and review, and will develop the necessary local internal procedures to implement its content, adapting it to any new regulatory developments that may occur, always in line with corporate policy and procedures.

5. Training

The necessary training and awareness-raising measures for data protection knowledge and culture shall be promoted and provided on a regular basis to increase the knowledge of employees, in particular those who have access to information systems.

6. Control and supervision

The Data Protection Officer will supervise compliance with the provisions of this Policy, in conjunction with the various Data Protection Coordinators designated at national and international level, who will be responsible for establishing and implementing internal procedures of a local nature, adapting their content according to the applicable law in their respective jurisdictions.

7. Doubts, communications or complaints

Queries within the scope of this Policy should be addressed to the Corporate Cybersecurity and Data Protection Department of URBASER at 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, should be addressed to the corresponding regulatory compliance body through the Ethics Channel set up on the Group's website (www.urbaser.com).

8. Non-compliance

This Policy is considered to be a mandatory rule, and therefore its violation will constitute a breach of it and the Company will adopt the appropriate disciplinary, contractual or legal measures, where appropriate, without prejudice to any other responsibilities that the offender may have incurred. Likewise, URBASER will reserve the right to adopt the measures that it considers appropriate against the business partners that do not comply with it. Any exception or exemption, whether for organisational, legal, contractual, technological or other reasons to this Policy or to any rule, procedure or technical instruction on which it depends, will be managed in accordance with the internal documents defined for this purpose.

9. Review and update

The Corporate Cybersecurity and Data Protection 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 Information Security Committee the modifications and updates that contribute to its development, approval and continuous improvement.

www.urbaser.com