Corporate Data Protection Policy

Chief Executive Officer
24 November 2025

VERSION CONTROL

Version	Date	Changes
V1	03/03/2023	New Creation
V2	29/10/2024	Content update
V3	24/11/2025	Grammar review

CONTENT

1. Purpose

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

In particular, the Policy guarantees the right to data protection for all individuals who interact with the companies 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 different sources and for different purposes depending on the business activity carried out.

2. Scope of Application

This document is mandatory for all investee entities (companies, joint ventures, joint ventures and other equivalent associations) in which URBASER, S.A.U. is the majority shareholder or has control, and is mandatory for all users who participate in the management, use or exploitation of personal data generated and processed at URBASER, including, but not limited to directors, executives, employees, collaborators, managers, members of governing bodies, all without prejudice to the specific legislation and legal requirements applicable in each country.

In those investee companies where this Policy does not apply, the alignment of their own policies with those of this Policy will be promoted through their representatives on the administrative bodies.

IMPORTANT: In the event that local or sectoral regulations contravene the provisions of this policy, each country or region must adapt it to the applicable legislation. All of this must be taken into account, given that this document sets out minimum guarantees in terms of data protection that must be respected at all times and cannot be modified in order to make them less effective.

3. Content

Principles and general considerations regarding the processing of personal data

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

Likewise, the principles and considerations set out 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 that involve the processing of personal data; and (iv) in the implementation of any systems and platforms that allow access by Group professionals or third parties to personal data and the collection or processing of such data.

In accordance with the above, any processing of personal data carried out within the Group must 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 legitimate, 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, an 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 the data subjects.

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

Likewise, personal data must be processed fairly and lawfully, which means that the entity cannot use it in a misleading or fraudulent manner.

Personal data relating to ethnic or racial 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 a person shall not be

collected or processed, unless there is legal authorisation in accordance with data protection regulations and/or applicable local regulations, in which case it must be proven that the processing is necessary, legitimate and proportionate, and that there are no alternative methods that can satisfy the same purpose.

b) Principle of minimisation

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

c) Principle of accuracy

Personal data must be accurate and up to date , and reasonable measures must be taken to enable the data subject to request its rectification or erasure where appropriate in each case.

d) Principle of purpose limitation and storage limitation

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

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 shall not be kept for longer than is necessary to achieve the purpose for which it was collected, except in cases provided for by law.

e) Principles of integrity and confidentiality

When processing personal data, adequate security measures must be taken, through technical and organisational measures, to protect it from unauthorised or unlawful processing and to prevent its loss, destruction and/or accidental damage.

Personal data collected and processed by Group entities must be kept strictly confidential and secret, and may not be used for purposes other than those that justified and permitted its collection, nor may it be communicated or transferred to third parties except in cases permitted by applicable law.

f) Principle of proactive responsibility (accountability)

The Group's entities shall be responsible for complying with the principles set out in this Policy and those required by applicable legislation and must be able to demonstrate this.

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

Likewise, a register or inventory of activities must be kept, describing the personal data processing carried out within the framework 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 a DPO, 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, providing them with information about the processing of their data in an understandable and accessible manner.

In order to ensure fair and transparent processing, the Group entity responsible for the processing shall inform the data subjects or interested parties whose data is to be collected, specifically:

- the identity and contact details of the data 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 may be exercised by the data subjects.
- the intention to carry out international transfers, if applicable;
- the data retention period;
- the contact details of the Data Protection Officer, if applicable.

h) Acquisition or collection of personal data

The acquisition or obtaining of personal data from illegitimate sources, from sources that do not sufficiently guarantee its legitimate origin, or from sources whose data has been collected or transferred in violation of the law is prohibited.

i) Hiring of data processors

Prior to contracting any service provider that has access to personal data for which the Group's entities are responsible, and throughout the duration of the contractual relationship, the necessary measures must be taken to ensure that an adequate level of security is provided.

Likewise, once an adequate level of security has been verified for the service provider that will have access to the information systems of any of the companies that make up the Group, the corresponding personal data processing and confidentiality contracts will be signed, where applicable.

j) International data transfers

When processing involves the international transfer of personal data to a third country or international organisation that does not offer the same level of guarantees, the necessary measures must be taken to reinforce the security of the personal data, so that it can only be carried out by establishing adequate guarantees.

Likewise, Group entities 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 data subjects

Group entities must allow data subjects to exercise their rights of access, rectification, erasure, restriction of processing, portability and objection as 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 and the internal procedures implementing it must be followed. Such incidents must be documented and measures must be taken to resolve and mitigate any negative effects on the data subjects.

m) Record of Processing Activities

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

In this way, all Group companies must maintain an inventory that includes, at a minimum, the set of processing activities, purposes and their corresponding description, type of data processed, and other issues 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 shall devote the appropriate resources to its implementation, maintenance and review, and shall develop the necessary local internal procedures to implement its content, adapting it to any new regulations that may arise, always in line with corporate policy and procedures.

5. Training

The necessary training and awareness measures will be promoted to raise knowledge and awareness of data protection, which must be provided on a regular basis to increase the knowledge of employees, particularly those who have access to information systems.

6. Control and supervision

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

7. Questions, communications or complaints

Any queries regarding this Policy should be addressed to URBASER's Corporate Cybersecurity and Data Protection Department at the following email address:pdp@urbaser.com .

Any incident relating to 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 relevant regulatory compliance body through the Ethics Channel provided on the Group's website (https://www.urbaser.com/canal-etico/).

8. Breaches

This Policy is considered a mandatory rule, and any violation thereof will constitute a breach of this Policy and the Company will take the appropriate disciplinary, contractual or legal measures, as applicable, without prejudice to any other liabilities that the offender may have incurred. Similarly, URBASER reserves the right to take any measures it deems appropriate against business partners who breach 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 current recommendations and best practices, and will propose to the Information Security Committee any modifications and updates that contribute to its development, approval and continuous improvement.

www.urbaser.com