

**COMPLIANCE POLICY REGARDING  
PERSONAL DATA PROTECTION AND  
PRIVACY**

**INDUSTRIA DE DISEÑO TEXTIL, S.A.**  
**(INDITEX, S.A.)**

**APPROVED BY THE BOARD OF DIRECTORS**  
**ON 11 JUNE 2019**

---

COMPLIANCE POLICY REGARDING  
PERSONAL DATA PROTECTION AND PRIVACY

Reference	
Name of the Standard	Compliance Policy regarding Personal Data Protection and Privacy
Scope	Global
Type	Policy
Supervisor	Data Protection and Privacy Department
Date of approval	2019/06/11
Version	1.0

**TABLE OF CONTENTS**

---

<b>1. Approval</b>	<b>4</b>
<b>2. Purpose</b>	<b>4</b>
<b>3. Scope of application</b>	<b>4</b>
<b>4. Contents of the Policy</b>	<b>5</b>
4.1 Definitions	5
4.2 Principles regarding personal data processing and commitments undertaken by the Company	6
<b>5. Responsibilities</b>	<b>7</b>
<b>6. Control and audit</b>	<b>8</b>
<b>7. Statement of compliance</b>	<b>8</b>

## 1. Approval

The Compliance Policy regarding Personal Data Protection and Privacy (the “**Policy**” or the “Data Protection Policy”) has been approved by the Board of Directors on 11 June 2019, following a favourable report of the Audit and Control Committee. Such Policy intertwines with the ethical values of the Inditex Group (hereinafter, “**Inditex**” or the “**Company**”) defined in the Code of Conduct and Responsible Practices (the “**Code of Conduct**”).

## 2. Purpose

This Policy seeks to lay down and standardize the level of compliance by all the companies within the Inditex Group with the most exacting regulations and best practices on personal data protection and privacy.

Likewise, this Policy implements the provisions of section 4.11 of the Code of Conduct regarding personal data protection, and is based in the entitlement – pursuant to the Compliance Policy – to prepare specific compliance policies that implement and extend the contents of the Compliance Policy and the Compliance Management Procedure.

This Policy is aligned with Inditex’s strategic objectives, and as such, demands the firm commitment of the management and of all the employees to comply with its provisions upon processing the personal data of the employees, candidates, customers, users, shareholders, suppliers and other data subjects.

Being a high-level regulation, this Policy allows preparing specific compliance internal regulations to implement and extend its contents (both procedures and instructions).

## 3. Scope of application

Compliance with this Policy is mandatory and it globally applies to all the companies within the Inditex Group. It shall be binding for the entire staff, regardless of their job and position.

For such purposes, Inditex Group shall mean any company in which Inditex owns, whether directly or indirectly, at least a 50% stake of the share capital or 50% of the voting rights.

The enforcement of this Policy, in full or in part, may extend to any natural and/or legal person associated with Inditex, where this may be appropriate to meet its purpose, and practicable on account of the nature of the relationship binding them with Inditex.

The Policy will be available to all employees on the corporate intranet (INET) and will be circulated to all Directors and Executives, as well as to anyone engaged in a contractual relationship with the Company, where this is required on account of the nature of the relationship, all of whom shall commit to complying with it.

The application of this Policy is supplementary to other mandatory internal regulations, such as the Information Security Policy and any others relating to Company’s information.

Under no circumstances may the application of this Policy and its implementing regulations entail any breach of the prevailing statutory provisions in force in the markets where Inditex operates. Such provisions shall always prevail over any internal regulation. In the absence of any effective statutory

provisions in the market corresponding to or supplementary to those existing, the contents of the Policy shall apply.

#### 4. Contents of the Policy

The provisions of this Policy are based upon the definitions, overarching principles and statutory requirements provided in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, ("**GDPR**").

##### 4.1 Definitions

For the purposes of a streamlined understanding of the personal data protection and privacy terms, the following terms shall have the following meaning:

- **Personal Data:** any information relating to an identified or identifiable natural person ("**Data subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Processing:** any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **Controller:** the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **Processor:** the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- **Recipient:** the natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.
- **Third party:** the natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data
- **Personal data breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- **Special categories of personal data:** such personal data which can only be processed when certain requirements laid down in the applicable regulations are met, as well as those which, given their special nature, the Company may consider as such at any time. Namely, the following:
  - Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;

- genetic data;
- biometric data;
- data concerning health;
- data concerning sex life or sexual orientation; and
- data relating to criminal convictions and offences.

#### 4.2 Principles regarding personal data processing and commitments undertaken by the Company

The principles that guide Inditex and the commitments undertaken regarding processing of personal data under the control of the Group are:

- **Lawfulness, fairness and transparency:** personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject so that they may be aware of the processing, as the case may be, of their data.
- **Purpose limitation:** personal data shall only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data minimization:** personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy:** personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- **Storage limitation:** personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Integrity and confidentiality:** personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. All the foregoing in accordance with applicable laws and with the provisions of mandatory internal regulations in the field.
- **Accountability:** shall be responsible for, and be able to demonstrate compliance with, the principles set out in this Policy, and in the applicable regulations on personal data and privacy.
- **Data Protection Officer:** in accordance with applicable regulations, and willing to follow best practices in the market, the Company shall endorse the Data Protection Officer (the “DPO”) and her team with regard to their duties of compliance with personal data and privacy regulations, and will make available to data subjects and authorities its contact details.
- **Data protection by design and by default:** the Company shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

- **Evaluation of risk and impact regarding personal data protection:** where any activity involving personal data protection is likely to entail a high risk to the rights and freedoms of data subjects, Inditex shall, to the extent and in the manner permitted by law, evaluate risk and impact on personal data protection and privacy prior to the start of processing activities.
- **Management of personal data breach:** in the event of a personal data breach, the corporate information security procedures shall be followed, as well as such specific procedures on personal data and privacy that cover management of notifications to the authorities and/or the data subjects.
- **Rights of the data subjects:** the Company shall ensure that data subjects are able to exercise such rights of access, rights to rectification, erasure, restriction of processing, data portability and the right to object, applicable in each jurisdiction, preparing for such purposes such internal regulations which are necessary to at least meet the requirements of the applicable regulations.
- **Hiring of service providers:** where service providers may have access to personal data under the control of Inditex:
  - Such access shall be restricted to strictly necessary personal data, exclusively;
  - The service provider shall be carefully selected. In particular, technical and organisational security measures provided shall be considered; and; y
  - The relationship between Inditex's company and the service provider shall be duly regulated by means of appropriate contractual terms on personal data processing.
- **International data transfers:** the Company shall meet the requirements laid down for international data transfers which are, as the case may be, applicable in the markets where it operates.
- **Records of processing activities:** Inditex shall maintain a record of processing activities under its responsibility whereby processing of personal data carried out in the framework of the Company's business are described, in accordance with applicable laws.

## 5. Responsibilities

Inditex Personal Data and Privacy Department, which is entrusted with Compliance functions in the areas of personal data and privacy, pursuant to the provisions of the corporate Compliance Management Procedure, shall be responsible for ensuring appropriate observance of this Policy. In particular, the DPO shall be responsible for advising and overseeing compliance with the regulations associated with the Policy. The DPO may rely on the collaboration of other areas or departments of the Company for the appropriate discharge of her duties.

Without prejudice to the generality of the foregoing, the Company shall be ultimately responsible for enforcing the applicable regulations and standards and as such, it shall ensure that compliance obligations in the field of personal data protection and privacy are ingrained in its day-to-day. This applies to the entire organisation, both to governing bodies and employees.

Inditex employees shall be responsible for complying with this Policy and with any implementing internal regulations. Namely, each employee shall:

COMPLIANCE POLICY REGARDING  
PERSONAL DATA PROTECTION AND PRIVACY

- comply, in the course of their activities, with their confidentiality and secrecy obligations regarding personal data to which they have access;
- use personal data exclusively for the purpose to which they were collected, in the scope of their working responsibilities;
- attend training sessions on privacy or data protection;
- assist with the implementation of measures and provide such information and documentation as may be requested to support compliance in the field of personal data protection and privacy; and
- disclose any noncompliance with this Policy by contacting either their supervisor or line manager, or directly the DPO and the Personal Data and Privacy Department at: [dataprotection@inditex.com](mailto:dataprotection@inditex.com);

**6. Control and audit**

Inditex will be subject to reviews, monitoring, and audits to assess general observance of this Policy.

**7. Statement of compliance**

Compliance with the principles and requirements laid down in this Policy is very often a statutory obligation or a standard. Therefore, the entire staff is expected to be familiar with this Policy and respect its contents. Likewise, with regard to third parties with whom Inditex is engaged in any business relationships, they are expected to behave in line with the provisions of the Policy.

Inditex shall forthwith react to any potential noncompliance with the provisions of this Policy, within the parameters of the applicable laws and regulations.

In addition, the Committee of Ethics and the Whistle Blowing Channel ensure compliance with this Policy. Any comments, queries or claims regarding the construction, application or enforcement of the Policy may be addressed to such bodies.

\*\*\*