\*\* FREE PREVIEW VERSION \*\*

[Organization logo]

[Organization name]

**PERSONAL DATA PROTECTION POLICY**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Date of version: |  |
| Created by: |  |
| Approved by: |  |
| Confidentiality level: |  |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| dd.mm.yyyy | 0.1 | EUGDPRAcademy | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 4](#_Toc114501072)

[2. Reference documents 4](#_Toc114501073)

[3. Definitions 4](#_Toc114501074)

[4. Basic principles regarding personal data processing 6](#_Toc114501075)

[4.1. Lawfulness, fairness and transparency 6](#_Toc114501076)

[4.2. Purpose limitation 6](#_Toc114501077)

[4.3. Data minimization 6](#_Toc114501078)

[4.4. Accuracy 7](#_Toc114501079)

[4.5. Storage period limitation 7](#_Toc114501080)

[4.6. Integrity and confidentiality 7](#_Toc114501081)

[4.7. Accountability 7](#_Toc114501082)

[5. Building data protection in business activities 7](#_Toc114501083)

[5.1. Notification to data subjects 7](#_Toc114501084)

[5.2. Data subject’s choice and consent 7](#_Toc114501085)

[5.3. Collection 7](#_Toc114501086)

[5.4. Use, retention, and disposal 7](#_Toc114501087)

[5.5. Disclosure to third parties 8](#_Toc114501088)

[5.6. Cross-border transfer of personal data 8](#_Toc114501089)

[5.7. Rights of access by data subjects 8](#_Toc114501090)

[5.8. Data portability 8](#_Toc114501091)

[5.9. Right to be forgotten 8](#_Toc114501092)

[6. Fair processing guidelines 9](#_Toc114501093)

[6.1. Notices to data subjects 9](#_Toc114501094)

[6.2. Obtaining consents 9](#_Toc114501095)

[7. Organization and responsibilities 10](#_Toc114501096)

[8. Guidelines for establishing the Lead Supervisory Authority 11](#_Toc114501097)

[8.1. Necessity to establish the Lead Supervisory Authority 11](#_Toc114501098)

[8.2. Main establishment and the Lead Supervisory Authority 11](#_Toc114501099)

[8.2.1. Main establishment for the data controller 11](#_Toc114501100)

[8.2.2. Main establishment for the data processor 12](#_Toc114501101)

[8.2.3. Main establishment for non-EU companies for data controllers and processors 12](#_Toc114501102)

[9. Response to personal data breach incidents 12](#_Toc114501103)

[10. Audit and accountability 12](#_Toc114501104)

[11. Conflicts of law 13](#_Toc114501105)

[12. Managing records kept on the basis of this document 13](#_Toc114501106)

[13. Validity and document management 14](#_Toc114501107)

# Purpose, scope and users

[Company name], hereinafter referred to as the “Company”, strives to comply with applicable laws and regulations related to personal data protection in countries where the Company operates. This Policy sets forth the basic principles by which the Company processes the personal data of consumers, customers, suppliers, business partners, employees and other individuals, and indicates the responsibilities of its business departments and employees while processing personal data.

This Policy applies to the Company and its directly or indirectly controlled wholly-owned subsidiaries conducting business within the European Economic Area (EEA) or processing the personal data of data subjects within EEA.

The users of this document are all employees, permanent or temporary, and all contractors working on behalf of the Company.

# Reference documents

* EU GDPR Article 24(2) of the EU GDPR 2016/679 (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, and repealing Directive 95/46/EC)
* [relevant national law or regulation for GDPR implementation]
* [other local laws and regulations]
* Employee Personal Data Protection Policy
* Data Retention Policy
* Data Protection Officer Job Description
* Guidelines for Data Inventory and Processing Activities
* Data Subject Access Request Procedure
* Data Protection Impact Assessment Methodology
* Cross-Border Personal Data Transfer Procedure
* [information security policies]
* Data Breach Response and Notification Procedure

# Definitions

The following definitions of terms used in this document are drawn from Article 4 of the European Union’s General Data Protection Regulation:

**Personal Data:** Any information relating to an identified or identifiable natural person ("**Data Subject**") 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.

**Sensitive Personal Data:** Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

**Data Controller**: The natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

\*\* END OF FREE PREVIEW \*\*

To download full version of this document click here: <https://advisera.com/eugdpracademy/documentation/personal-data-protection-policy/>