\*\* FREE PREVIEW VERSION \*\*

[organization logo]

[organization name]

**EMPLOYEE PERSONAL DATA PROTECTION POLICY**

|  |  |
| --- | --- |
| Code: |  |
| Version: | 1 |
| 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](#_Toc496533361)

[2. Reference documents 4](#_Toc496533362)

[3. Definitions 4](#_Toc496533363)

[3.1. Personal Data 4](#_Toc496533364)

[3.2. Sensitive Personal Data 4](#_Toc496533365)

[3.3. Processing 5](#_Toc496533366)

[3.4. Data Controller 5](#_Toc496533367)

[4. General Principles for Processing Employee Personal Data 5](#_Toc496533368)

[4.1. Lawfulness, fairness, and transparency 5](#_Toc496533369)

[4.2. Purpose limitation 5](#_Toc496533370)

[4.3. Data minimization 5](#_Toc496533371)

[4.4. Accuracy 5](#_Toc496533372)

[4.5. Storage period limitation 5](#_Toc496533373)

[4.6. Integrity and confidentiality 6](#_Toc496533374)

[4.7. Accountability 6](#_Toc496533375)

[5. Legitimate Purposes for Processing Employee Personal Data 6](#_Toc496533376)

[6. Requirements for the Processing of Employee Personal Data 6](#_Toc496533377)

[6.1. Notification to Employees 6](#_Toc496533378)

[6.2. Employee Choice and Consent 7](#_Toc496533379)

[6.3. Collection 7](#_Toc496533380)

[6.4. Use, Retention, and Disposal 7](#_Toc496533381)

[6.5. Disclosure to a Third Party 8](#_Toc496533382)

[6.6. Cross-border Transfer of Employee Personal Data 8](#_Toc496533383)

[6.7. Employee Access 8](#_Toc496533384)

[7. Responsibilities 8](#_Toc496533385)

[8. Response in the Event of Non-compliance 9](#_Toc496533386)

[9. Accountability 9](#_Toc496533387)

[10. Exceptions and Variations 9](#_Toc496533388)

[11. Owner and Contacts 9](#_Toc496533389)

[12. Managing records kept on the basis of this document 9](#_Toc496533390)

[13. Validity and document management 10](#_Toc496533391)

# Purpose, Scope and Users

This Policy regulates the management of Personal Data relating to the employees of [company name] (“The Company”), and provides rules and procedures which apply to all departments and individuals within the Company, aimed at ensuring that employee Personal Data is processed and protected properly in all countries and regions.

This Policy applies to the Processing of employee Personal Data by any department or individual within the Company, in all countries and regions.

"Company" refers to [company name] and all wholly-owned subsidiaries directly or indirectly controlled by it; but excludes joint venture companies.

The users of this document are all employees of The Company.

# Reference documents

* 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]
* Personal Data Protection Policy
* Data Retention Policy
* Data Breach Policy
* Cross Border Data Transfer Policy
* Data Breach 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 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, mental, economic, cultural, or social identity of that natural person. Personal Data includes a natural person's email address, telephone number, biometric information (such as fingerprint), location data, IP address, health care information, religious beliefs, Social Security number, marital status, et cetera.

## Sensitive Personal Data

Particularly sensitive in relation to fundamental rights and freedoms, where disclosure of such data could lead to physical damage, financial loss, damage to the reputation, identity theft or fraud or discrimination etc. Sensitive personal data usually includes but not limited to personal data revealing racial or ethnic origin, political opinion, religious or philosophical belief, or trade union membership, as well as genetic data, biometric data (fingerprint) for the purpose of uniquely identifying a natural person, and data concerning a natural person's health, sex life or sexual orientation.

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

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