|  |
| --- |
| Attachment no. Add number here |
| Write name of attachment here |
| Date: 2023-02-09 |
| Document security: Internal |

# General Data Protection Policy

### Enento Group, February 9th, 2023

1. **Purpose**

This General Data Protection Policy focuses on the legal requirements established by the General Data Protection Regulation ("GDPR"). Where local Data Protection law establishes greater protections for Personal Data, such local law applies. This General Data Protection Policy implements the core principles of the GDPR and aims to establish and standardize a group-wide level of Data Protection Compliance.

Data Protection laws such as the GDPR build on the principles of free flow of Personal Data and the protection of Personal Data. Finding the right balance between these two principles is of fundamental importance for Enento Group as many different stakeholders trust us in processing their data as well as relying on us when using our services. It is also recognized that Data Protection Compliance is a vital component for Enento Groups competitiveness in the market.

1. **Target group**

This General Data Protection Policy has been implemented by each affiliate and subsidiary of the Enento Group (each affiliate or subsidiary referred to as "Company") in order to establish a Group wide standard for the protection of any Personal Data when processed by members of the Enento Group. The employees, contractors, consultants and agents of the Company ("Employees") are obliged to comply with this General Data Protection Policy whenever the Employees process Personal Data in connection with or in the context of the performance of their job responsibilities for Company. This General Data Protection Policy does not create any rights outside the scope of the Company’s obligations under applicable law. This General Data Protection Policy is confidential and internal to the Company and shall not create any rights or entitlements of any Employee or third parties.

This General Data Protection Policy is applicable to the processing of Personal Data by Company both when Company acts as Processor and/or Controller. The responsibilities and duties as a Processor are however not the same as when Company is Controller.

1. **Definitions**

Capitalized terms shall have the meaning given below throughout this General

Data Protection Policy.

**Data Subject** means a natural person to which Personal Data relate

**Controller** means a Company, acting alone or jointly with others, determining the purposes and means of processing of Personal Data

**GDPR** means General Data Protection Regulation

**Processor** means a Company processing Personal Data on behalf of the Controller

**Personal Data** means any information relating to an identified or identifiable natural person. 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 (e.g., IP-address, cookie tag) or location data. The term Personal Data is very broad under the GDPR. To qualify as Personal Data it is not necessary to combine the name of a natural person with other identifiers of the natural person. See also point 4. for examples

**Processing** means any use or operation which is performed on Personal Data. That means, anything one can do with Personal Data, such as collection, recording, organizing, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, transfer or otherwise making available, alignment or combination, restriction, erasure or destruction. Please note that processing can include asking a person for information, capturing information on call details (including call recording), logging and analysing network traffic and accessing a customer’s CRM system or other external database.

1. **Personal Data**

Personal Data may include:

• Employee Personal Data, for example, master data (e.g. social security number, name, address, phone number, e-mail address, citizenship, marital status), organizational data (e.g. org. unit, cost center, personnel number, employee manager), contractual data (e.g. employment status, contract type, average working hours), compensation and benefit information, employee attendance data (e.g. time records, paid time off), performance and talent information (e.g. CV, training, performance ratings, discipline), information about Company assets assigned and used to employee (type of laptops, mobile phone etc., IT-usage data), information contained in emails and other business communication;

• Applicant Personal Data, for example, contact details, CV information, work and education history, skills;

• Business Partner/Vendor Personal Data (in case of natural persons or staff members of Business Partners/Vendors), for example, contact details, information contained in emails and other business communication, bank account details, CRM activities;

• Website/Application User Personal Data, for example, IP-address or other online identifiers, location data, log-file data, contact details.

• Credit information Personal Data and business information Personal Data allowed in accordance with local legislation and permits. It varies from country to country but the processing may entail large quantities of Personal Data, for example, social security number/business identity number, name, address, income statements, credits- and misuse of credits, financial data, marital status, default information, and also more sensitive data such as health records or fraud/block of identity information, protected addresses, etc.

1. **Special Categories of Personal Data**

Special Categories of Personal Data or also called sensitive data are Personal Data which may only be processed under further requirements. Special Categories of Personal Data are:

• Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;

• Genetic data;

• Biometric data (such as electronic fingerprint or iris scan) when processed for the purpose of uniquely identifying a natural person;

• Data concerning health (such as employee disability status or medical history);

• Data concerning a natural person's sex life or sexual orientation.

1. **Core Data Protection Requirements**

The Company and each of its Employees need to ensure that they always comply with the following Core Data Protection Requirements when processing Personal Data. ‘

* 1. **Data Processing Principles**

Each Employee must ensure that Personal Data is

(i) Processed lawfully, fairly and in a transparent manner in relation to the Data Subject (‘**lawfulness, fairness and transparency’**);

(ii) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (‘**purpose limitation**’);

(iii) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘**data minimisation**’);

(iv) 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 (‘**accuracy**’);

(v) 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 unless specifically authorized by law; (‘**storage limitation**’);

(vi) 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 (‘**integrity and confidentiality**’).

* 1. **Legal Basis for Processing Personal Data**

The Company shall only process Personal Data (including making available to others (including other Enento affiliates or subsidiaries)) where a legal basis permits the processing of the Personal Data. General legislation such as the GDPR (lex generalis) clarifies that processing of Personal Data is only lawful to the extent at least one of six legal bases are applicable. The six legal bases are specified in article 6 of the GDPR. More specific legislation (lex specialis), such as for example local credit information acts or constitutional laws, may be applicable and as such clarify the legal basis for the processing of Personal Data. Please contact Group Legal or Data Management if you need assistance with determining the applicable legal basis.

* 1. **Data Subject Rights**

The Data Subjects whose Personal Data is processed by the Company have certain rights. Data subjects have

1. right to information;
2. right to access their Personal Data;
3. right to request rectification of their Personal Data;
4. right to request restriction of processing of their Personal Data;
5. right to request erasure of their Personal Data;
6. right to portability of their Personal Data;
7. right to object to the processing of their Personal Data (including profiling) and
8. rights related to automated decision making.

Data subject´s right to information is covered by notifying Data Subjects prior to the processing (see 6.4).

In case the Company receives a request concerning the other rights, the Company and its Employees must follow the Data Subject Rights Instruction.

* 1. **Privacy notice**

Where applicable, the Company acting as Controller must notify the Data Subjects prior to the processing with the following information:

• Identity of the Company responsible for the processing of the Personal Data (including contact details);

• Contact details of the Enento Group Data Protection Officer (where applicable);

• Types of Personal Data being processed;

• Purposes for the processing of the Personal Data as well as the legal basis (Legal Basis for processing Personal Data);

 • Where processing is based on the overriding legitimate interest of the Company as statutory justification ground, details on such legitimate interests;

• Recipients or categories of recipients of the Personal Data, International Data Transfers and reference to the appropriate safeguards and the means by which the Data Subject can obtain a copy of them or where they have been made available;

• Retention period of the Personal Data or criteria used to determine that period;

• Data Subject Rights under applicable Data Protection law, which may include the right of access, the right of erasure, or the right to object;

• Right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal;

• Right to lodge a claim with the competent supervisory authority;

• Whether the provision of Personal Data by the Data Subject is a statutory or contractual requirement or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences if the Data Subject does not provide such Personal Data,

• Existence of automated decision-making, including profiling, and meaningful information about the logic behind involved, the significance and the envisaged consequences of such processing for the Data Subject (which must be given in a clear and transparent way).

* 1. **Confidentiality**

All Employees must be committed to keeping any Personal Data confidential and not to disclose any Personal Data to unauthorized third parties (within the Company or outside of the Company). All Employees must sign a Confidentiality undertaking.

* 1. **Disclosure to Service Providers**

Service Providers (external third parties as well as Company's affiliate providing services to Company) may have access to Personal Data. In this case, Company must ensure that

1. such access is limited to the Personal Data which is absolutely necessary (need-to-know-principle);
2. the Service Provider is diligently chosen, considering in particular the technical and organizational security measures provided by the Service Provider, adherence to a recognized Code of Conduct for Data Protection or an approved Certification for Data Protection, and
3. appropriate Data Processing Clauses contained in a relevant service agreement or a separate Data Processing Agreement is in place.
	1. **Security/Safeguards**

The Company will take reasonable measures to ensure that Personal Data in the Company's possession and control are protected against loss, unauthorized access, use, destruction, modification or disclosure and ensure that appropriate technical and organisational security safeguards are in place to protect Personal Data appropriate to the level of risk and sensitivity of the data. Taking into account state-of-the-art, costs, nature, scope, context and purposes of Data processing as well as the rights and freedoms of the Data Subjects, this will when necessary include in particular the pseudonymization and encryption of Personal Data, measures to ensure confidentiality, integrity, availability and resilience, measures to restore the Personal Data in a timely manner in the event of an incident, and processes for regularly testing, assessing and evaluating the effectiveness of the security measures.

* 1. **International Data Transfers**

Personal Data must not be transferred to countries that do not provide an adequate level of Data Protection from a European Data Protection law perspective ("Restricted Countries") unless such transfer complies with the requirements of the GDPR.

Restricted Countries are any countries outside of the EU/EEA, however except where the European Commission has decided that certain countries offer an adequate level of Data Protection.

(See the complete list of adequacy decisions here <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> )

* 1. **Data Protection Impact Assessment/Data Protection by Design and by Default**

Where a processing activity, in particular implementing a new technology or IT system, is likely to result in a high risk to the rights and freedoms of the Data Subject, taking into account in particular the nature, scope, context and purpose of the envisaged processing activity, a Data Protection Impact Assessment must be carried out prior to the launch of the processing activity. The responsible Business Area or Functional Unit shall be responsible to perform Data Protection Impact Assessment. The level of Company's responsibility for such processing activities is limited if the processing activities are carried out by Company as Processor, i.e. on behalf of a Controller.

When developing or considering a new processing activity, in particular implementing a new technology or IT system, or changing any existing processing activities, appropriate technical and organizational security measures must be considered prior to implementation. By default, only Personal Data which is necessary for the intended purpose may be collected, processed and used. The level of Company's responsibility for such processing activities is limited if the processing activities are carried out by Company as Processor, i.e. on behalf of a Controller.

* 1. **Keeping Documentation up-to-date**

When developing or considering a new processing activity, in particular implementing a new technology or IT system, or changing any existing processing activities, the Employee shall act in accordance with the procedural descriptions outlined in the Quality Management System (“QMS”) or by our Group wide processes defined as part of Our Way in order to keep the related Data Protection documentation (such as Privacy notices, Data Protection Impact Assessment, Records of Processing Activities, Data Processing and Data Transfer Agreements) up-to-date.

* 1. **Records of Processing Activities**

The processing activities must be documented in a Record of Processing Activities. Each Business Area and Functional Unit is responsible for providing Group IT/Data Management with information and it is Group IT/Data Managements responsibility to make sure the completeness and accuracy of the Records of Processing Activities on a Group wide and on a local level.

* 1. **Data breaches**

All Employees are responsible for internally reporting a potential Data breach they have noticed or been informed of by a Processor of a Company. After reporting the Company is responsible for investigating and documenting all Data breaches internally according to the Data breach Reporting Instruction.

* 1. **Data Protection Governance Structure**

The Company is part of the Data Protection Governance Structure for compliance with Data Protection requirements. The Data Protection Governance Structure is established by the Data Protection Governance Policy.

* 1. **Awareness and Training**

All Employees will receive the basic Data Protection awareness training.

GDPR Basic training is mandatory to all Employees and shall be repeated on a yearly basis. In addition voluntary GDPR nanolearnings will be published concerning different Data Protection related topics.

All Employees are informed and instructed to become familiar with this General Data Protection Policy, the Data Protection Governance Policy and, as appropriate and relevant, other policies, instructions and guidelines.

1. **Responsibilities of all Employees**

All Employees of the Company are responsible for complying with this General Data Protection Policy, the Data Protection Governance Policy and, as appropriate and relevant other policies, instructions and guidelines.

In particular, each Employee shall:

1. meet his or her confidentiality obligations with respect to Personal Data;
2. process Personal Data only to the extent necessary to serve the legitimate purpose and to properly perform his or her responsibilities;
3. undertake any function-related or assigned Data Protection training;
4. promptly report any breach of the General Data Protection Policy by contacting his or her direct or functional manager or Group Legal.
5. report a potential Data breach they have noticed or been informed of by a Processor of a Company.

Failure to meet these responsibilities may result in loss of access privileges and/or disciplinary sanction up to and including termination to the extent permitted by applicable law.

1. **Additional information**

Any questions relating to the General Data Protection Policy should be directed to Data Protection Governance Manager.

This Policy is reviewed annually and is updated by Enento when necessary, changes are approved by the Audit Committee of Enento Group.

Effective Date: 2020-01-13

Latest version: 2023-02-09