Data Protection Policy

For all employees and external consultants of Emento

Versioning

Version	Date	Description	Author
1.0.0	13.08.2019	First version	Lyng Salling
1.0.1	10.09.2024	New typography and graphics, minor changes in wording	Tilde Holst Aaen

Authorisation

Date	Authorised by	Signature
09.09.2025	Allan Juhl, CEO	AJU

Table of Contents

1. Purpose

This policy aims to ensure the responsible and sustainable use and protection of data in accordance with applicable law and with respect for the rights of the data subject.

Emento's data protection policy is based on the data ethics principles and applies to all employees and external consultants of Emento.

2. The Definition of Data Ethics

Data ethics is the responsible and sustainable use of data. It is the "right" thing to do for people and society. Data processes should be designed as sustainable solutions, which can be maintained and verified, and should first and foremost be for the benefit of the individual.

Data ethics is about fulfilling the principles and values on which human rights and data protection law are based. It is about honest and genuine transparency in data management. It is about actively developing privacy by design and privacy-enhancing products and structures. About treating other people's personal data as you would want your own - or your children's - to be treated.

Data ethics goes beyond compliance with personal data legislation: all data processes therefore respect, as a minimum, the requirements set out in the EU General Data Protection Regulation (GDPR), the EU Charter of Fundamental Rights and the European Convention on Human Rights.

2. Data Ethics Principles

2.1. Putting people first

Human interests always take precedence over institutional and commercial interests. People are not computers or processes or pieces of software, but unique with human empathy, will, unpredictability, intuition and creativity, and people have a higher status than the machine. The person is at the centre and has the primary benefit of the data processing.

We must therefore ask ourselves the following:

- *Is our data processing organised on the basis that we borrow data from users?*
- *Do we ensure that user rights are prioritised over commercial or institutional interests?*
- *Are we ensuring that users get the most value from their own data - not just the organisation?*
- *Do we use privacy by design principles and can we describe them clearly and transparently?*

2.2. Individual data control

People have individual data control and agency. The autonomy of the individual is prioritised in all data processes and each person takes an active part in the data recorded about them. The individual has primary control over what their data is used for and in what contexts, as well as how their data is activated.

We must therefore ask ourselves the following:

- Profiling
  - *Do we use profiling? And do we allow the user to influence and determine the values, rules and inputs that underpin profiling?*
- Predictions
  - *Do we use data to predict behaviour at the individual level or only for patterns?*

2.3. Transparency

Data processing and automated decisions must make sense to the individual. They must be transparent and explainable. The purposes and interests of data processing must be transparent to people in terms of understanding risks, as well as social, ethical and societal consequences.

We must therefore ask ourselves the following:

- Data storage
  - *In which country is the data stored?*
  - *Where is the storage solution provider based?*

    - *Does the transmission of data go through countries outside the EU?*
- Artificial Intelligence
    - *Do we use machine learning/artificial intelligence? If so, can we explain our algorithm - the criteria and parameters?*
- Behavioural design
    - *Do we use personal data to influence behaviour?*
    - *Are we ensuring that it is transparent to users that their behaviour is being affected?*
    - *Do we ensure that the design does not create dependency and thus remove the individual's autonomy and agency?*
- Open source
    - *Do we operate with open ecosystems (open source software) so that others can use it and possibly work on it?*

2.4. Accountability

Accountability is one of Emento's core values and involves the conscious, objective and systematic use and protection of personal data. Responsibility and accountability are involved at all stages of data processing, and active efforts are made to minimise risks to the individual and to contain social and ethical consequences. Sustainable personal data processing is embedded throughout the organisation and ensures ethical accountability in the short, medium and long term. Emento's accountability also applies to subcontractors and partners.

We must therefore ask ourselves the following:

- Anonymity
    - *When do we anonymise personal data?*
    - *Do we use end-to-end data encryption?*
    - *Do we minimise the use of metadata and explain how?*
- Zero-knowledge
    - *Do we use zero-knowledge as a design and treatment principle?*
- Sale of data
    - *Do we sell data to third parties?*
    - *Do we sell data as personal data?*
    - *Do we sell data as patterns in aggregate form?*
    - *If we sell data, do we ensure that the data is fully anonymised and only describes patterns, not individuals?*
- Data sharing

    - *Do we use third-party cookies?*
    - *Do these include SoMe (social media) cookies and SoMe logon?*
    - *Do we use Google Analytics or similar tracking tools?*
    - *Are our users fully aware that our cookie use means that we share data about them with third parties and agree to this?*
- Data enrichment
    - *Do we enrich data with external data, e.g. from social media or web-scraping?*
    - *Is this enrichment at the request of or in collaboration with our users?*
- Organisational anchoring
    - *Do we have a person or entity responsible for the ethical handling of data?*
    - *How is the work with data ethics anchored in the organisation?*
    - *How do we ensure compliance with our data ethics guidelines?*
- External control
    - *Can the data processing be audited by an independent third party?*
    - *Do we require and check the data ethics of our subcontractors and partners?*

2.5. Equality

Democratic computing is based on the fact that data systems help to maintain, reproduce and create the distribution of power in society. Data processing must take particular account of vulnerable people who, for example, because of their economic, social or health circumstances, are particularly exposed to profiling that may have a negative impact on their autonomy and control, or expose them to discrimination or stigmatisation. Consideration of vulnerable people also means working actively to reduce bias in the development of self-learning algorithms.

We must therefore ask ourselves the following:

- Public platforms
    - *Do we have dialogue with our users on a public platform?*
    - *Do we have guidelines for using the platform?*
    - *Do we moderate the platform to remove sensitive personal data?*
    - *If we provide services to children etc, do we ensure parental consent?*
- Recycling
    - *Is data used to develop or train an algorithm?*

    - *Do we ensure that the use of data does not lead to discrimination?*
    - *Do we ensure that the use of data does not lead to the exposure of vulnerabilities in individuals?*
- *Artificial Intelligence*
    - *Do we ensure that the use of artificial intelligence/machine learning is beneficial to the individual and does not cause physical, psychological, social or economic harm to the individual?*

These principles are continuously incorporated into all relevant policies, procedures and processes and as a core part of the culture of Emento.