DATA ETHICS POLICY

MapUs / Center for Digital Dannelse

JUNE 2024

Date: June 6, 2024
Version: 1

Contact information:

Jacob Brøndum
Founder and CEO
jacob@digitaldannelse.org

Anders Skov
Founder and DPO / CTO
anders@digitaldannelse.org

Content

1. Introduction and Purpose **4**
2. Compliance with Laws and Regulations **5**
3. Responsible Data Processing **5**
3.1 Consent 5
3.2 Data Minimization 5
3.3 Guidelines for Data Access 5
3.4 Storage and Deletion of Data 5
3.4.1 If a Data Subject Requests Deletion 6
4. Data Protection and Security **6**
4.1 Information Security 6
4.2 Anonymization and Pseudonymization 6
4.3 Reporting Data Breaches 6
5. Transparent Communication **6**
6. Data Ethical Considerations **7**
7. Education and Awareness Activities **8**
8. Third Party Agreements **8**
9. Review and Revision **8**

1. Introduction and Purpose

At Center for Digital Dannelse, we are committed to upholding the highest standards of data ethics, ensuring that our data practices align with our values of responsibility, transparency, fairness, privacy, integrity, and accountability. This Data Ethics Policy is designed to articulate our dedication to ethical and responsible data processing, reflecting our compliance with applicable laws and regulations such as the General Data Protection Regulation (GDPR), the Danish Data Protection Act, and the E-Privacy Regulation.

Our approach to data ethics as well as the compilation of this policy are guided by international standards ISO/IEC 38500 and ISO 26000. We take these standards into consideration where we can to ensure commitment to social responsibility, environmental sustainability, and robust IT governance.

This policy is compiled to describe our commitment to respecting employee's privacy and protecting their data. By adhering to our Data Ethics Policy, we strive to maintain trust and respect with our customers, users, and stakeholders by ensuring their data is processed in a responsible, secure and ethical manner.

This policy will be reviewed and updated annually to reflect evolving legal requirements, technological advancements, and societal expectations, ensuring that our data practices remain ethical, effective, and aligned with our organizational values and international standards. At the beginning of the document, a revision history is provided to help clarify when review last took place.

2. Compliance with Laws and Regulations

Center for Digital Dannelse collects and processes data in accordance with applicable data protection laws and regulations, including but not limited to the General Data Protection Regulation (GDPR), the Danish Data Protection Act, and the E-Privacy Regulation. This ensures that our data processing complies with relevant legal requirements and standards.

3. Responsible Data Processing

3.1 Consent

We obtain consent from affected parties before processing their personal data, unless the processing is based on another valid legal basis.

3.2 Data Minimization

We commit to collecting and processing only the necessary data to fulfill our legitimate purposes. We avoid unnecessary data collection to ensure mutual trust with customers and suppliers.

3.3 Guidelines for Data Access

Data access is limited to authorized employees who need the data to perform their job duties. Access is managed and logged to ensure data protection. A documented overview of employees' administrative access is regularly updated, especially during new hires or resignations.
Customer data access is limited to authorized users who collect and need data for their use of the services provided by our organization. Access is managed and logged to ensure data protection.

3.4 Storage and Deletion of Data

We store data for the time necessary for our purposes and delete it when it is no longer relevant. Storage times comply with applicable laws. We respect individuals' rights to control and manage their own data and offer appropriate options for accessing and deleting personal data.

We comply with the following deletion deadlines for stored data:

Deleted after 5 years:

- Terminated subscriptions and customers who have not purchased presentations in the past five years.

Deleted after 3 years:

- Personal mappings in MapUs (individuals).

Deleted after 1 year:

- Terminated newsletter recipients, Slido polls, content in competency wheels for terminated subscribers anonymized

Deleted immediately after use:

- Child certificates and job and internship applications

3.4.1 If a Data Subject Requests Deletion

When a data subject requests deletion, we must:

1. Acknowledge receipt of the request via email
2. Delete the person's data in all systems where it is stored - unless it falls under the accounting law. In such cases, we are required to keep data for five years
3. Send an email back when all data is deleted - remember to delete the correspondence with the data subject afterward

4. Data Protection and Security

4.1 Information Security

We implement technical and organizational measures to protect data against unauthorized access, loss, or misuse, detailed in the company's policy on "Technical and Organizational Measures."

4.2 Anonymization and Pseudonymization

When appropriate, we anonymize or pseudonymize data to protect individuals' identities and our customers' information.

4.3 Reporting Data Breaches

We have procedures in place to identify, report, and handle data breaches or security incidents. Our IT emergency plan ensures that the Center for Digital Dannelse can maintain its critical functions and protect sensitive information in the event of IT incidents. It is crucial for us to respond quickly and effectively to potential threats, disruptions, and security breaches that may affect our operations and our customers' trust.

5. Transparent Communication

We communicate clearly with affected parties about how their data is collected, processed, and used. This includes informing about the purpose of data processing and any third-party agreements, especially through our privacy policy.

6. Data Ethical Considerations

Center for Digital Dannelse commits to handling data ethically and responsibly, going beyond the requirements of laws such as GDPR. Our data ethical considerations are not only based on legal compliance but also take into account broader implications for individuals, the environment, and society.

Considerations for the Individual
When collecting and processing data, we respect individuals' rights. We prioritize transparency, consent, and privacy. We inform users clearly and transparently about what data is collected, why, and how it is used and stored. We ensure that data collection occurs with informed and voluntary consent. Likewise, we implement strong technical and organizational measures to protect personal data against unauthorized access, loss, or misuse.

Considerations for the Environment
In relation to data minimization, we only collect necessary data to reduce storage needs and energy consumption in data processing. We also have requirements for regularly deleting

unnecessary data, especially in our individual mailboxes, to reduce storage.
We also make extensive use of recycling, particularly by reusing old computers to ensure sustainability and reduce environmental impact.

Considerations for Society
Data plays a central role in society, and we recognize a responsibility to design our technologies and services with a focus on creating value for users, ensuring usability, accessibility, and utility. We promote a culture of ethical innovation in the company, where new technologies are developed with the aim of promoting broader formation in the population.

To integrate these data ethical considerations into our practice, we include considerations for people, the environment, and society in our risk assessments. This means that when we assess risks related to data collection and processing, we focus not only on legal and technical consequences but also on how risks can have ethical and societal implications; such as how it can impact our customers if their data is compromised. We work proactively to identify and mitigate potential harms, and when an unwanted event occurs, we have an IT emergency plan and action cards ready to stop and limit the damage. Likewise, we have an anti-bribery policy to ensure that data handling is done in a way that promotes transparency, integrity, and accountability.

7. Education and Awareness Activities

We ensure that our employees and partners are educated and aware of the importance of data ethics and their responsibilities in data processing. Additionally, we have an annual "Digital Safety Day", where we address these topics and work problem-based with a range of dilemmas to ensure that all employees are knowledgeable about correct data handling and processing.

8. Third Party Agreements

We only enter into agreements with reliable third parties that meet our standards for data processing and data protection. Written agreements are established with appropriate data processor agreements.

9. Review and Revision

We regularly review and update our data ethics policy to ensure it complies with legislation and business needs.

Revision history

Date	Version	Comment	Author
28.07.2023	1.0	Data Ethics Policy created	LWP, JB
28.05.2024	1.0	Data Ethics Policy revised and updated	ERH, LVSV
04/08.2025	1.0	Data Ethics Policy revised and updated	MAH