Data Ethics Policy

Purpose
This policy outlines our commitment to ethical and responsible data practices in compliance with the General Data Protection Regulation (GDPR). Our objective is to ensure that the personal data of our users and customers are processed lawfully, fairly, and transparently.

Company Objectives
Our company's data ethics policy is guided by the following objectives:

- To protect the privacy and personal data of our customers, employees, and partners.
- To comply with all relevant data protection laws, including GDPR and other applicable regulations.
- To ensure transparency and accountability in our data processing activities.
- To minimize the collection and use of personal data to the extent necessary for business purposes.
- To promote awareness and understanding of data ethics among our employees, contractors, and partners.

Scope
This policy applies to all employees, contractors, partners, and third-party service providers who collect, process, or store personal data on behalf of our organization.

Principles of Data Ethics
We commit to the following principles of data ethics:

Lawfulness, fairness, and transparency
We collect, process, and store personal data in a lawful, fair, and transparent manner. We will obtain consent from the data subjects before processing their personal data and provide clear and concise information about the purpose and nature of data processing.

Purpose limitation and data minimization
We collect and process personal data only for specific, explicit, and legitimate purposes. We will ensure that the personal data collected are relevant, adequate, and limited to what is necessary for the intended purpose.

Accuracy and integrity
We will ensure that personal data collected are accurate and kept up-to-date. We will also take appropriate measures to ensure the integrity, confidentiality, and security of the personal data.

Data subject rights
We respect the rights of data subjects, including the right to access, rectify, erase, restrict processing, and object to the processing of their personal data. We will respond promptly to any data subject requests and ensure that their rights are upheld.

Accountability
We take responsibility for our data processing activities and have appropriate policies and procedures in place to ensure compliance with GDPR. We will also regularly review our data processing activities to identify and mitigate any risks to data subjects.

Data Protection Officer (DPO)
We have appointed the Operations & Privacy Officer to oversee our data protection practices and ensure compliance with GDPR. The Operations & Privacy Officer is the main point of contact for any data protection-related issues and can be reached at privacy@intellifinder.dk

Product Development and Operations
In our product development and general operations, we consider data ethics beyond GDPR and data protection laws. We prioritize the privacy and data protection of our users by making conscious choices to limit data collection and ensure privacy by default.

We also consider the following aspects in our product development and operations:

Ethical Use of Data
We ensure that the data collected is used ethically and responsibly. This includes avoiding using personal data for purposes that could harm individuals or lead to discriminatory practices.

Data Security
We implement robust security measures to safeguard the personal data we collect, process, and store. This includes encryption, access controls, and regular security assessments.

Data Anonymization and Pseudonymization
Wherever possible, we anonymize or pseudonymize personal data to protect the privacy of individuals.

Data Sharing and Third-Party Vendors
We carefully assess the data privacy practices of third-party vendors and partners before sharing personal data with them. Contracts with third-party vendors include data protection clauses to ensure the responsible handling of personal data.

Data Breach Management
In the event of a data breach, we will take immediate action to contain the breach, assess the risks to data subjects, and notify the relevant supervisory authority and data subjects as required by GDPR.

Implementation
To implement this policy effectively, the following steps will be taken

Training and Awareness
We provide regular training and awareness programs to all employees, contractors, partners, and third-party service providers who handle personal data on behalf of our organization. The training covers GDPR requirements, our data ethics policy, and the importance of data protection.

Data Protection Impact Assessment (DPIA)
For projects or processes involving high-risk data processing, a Data Protection Impact Assessment (DPIA) will be conducted to identify and mitigate potential risks to data subjects' rights and freedoms.

Data Retention
We will establish clear data retention policies and ensure that personal data is retained only for as long as necessary for the specified purposes.

Reporting to Management
The Operations & Privacy Officer will provide periodic reports to the management team on data ethics, including:

- An overview of data protection measures and compliance efforts.
- Updates on data protection impact assessments (DPIAs) and risk management.
- Any incidents of data breaches or non-compliance and the actions taken to address them.

Review and Update
We will review and update our data ethics policy periodically to ensure that it remains compliant with GDPR and reflects any changes in our data processing activities.

Updated July 2024