December 2024

Data ethics policy

Introduction

We live in an age where new digital processes and new technology are continuously available to us. This presents opportunities to increase our knowledge and improve our services to customers and business partners. The fuel in the new processes and technologies is, as a rule, data, and it is therefore central for Visma DataLøn and ProLøn A/S (hereafter Visma/we/us) to focus on the responsibility that falls on us when we carry out data processing.

It is crucial that our customers and business partners can trust us and be comfortable with our handling of data. Therefore, we have a strong focus on:

- assessing risks, address them and thereby maintain a high level of information security,

- complying with agreements and legislation, including personal data rights,
- determining and following our internal ethical rules in order to maintain this trust both in relation to the individual person or company and in relation to society.

This policy is Visma DataLøn and ProLøn A/S' ethical rules for processing data.

Data Ethics

Ethics is doing the right thing - even if no one is looking. It is usually our core values that guide us. Everyday life is full of situations that call for an ethical consideration. When you act ethically, you don't just try to satisfy yourself and your own interests, but also take into account what is the good and right thing to do in the specific situation - both in relation to the individual person, a concrete company and society.

Data ethics must be understood as the part of ethics that concerns the use of data, not only personal data but also data not governed by the GDPR, including data about B2B relations, aggregated and anonymized data.

Data ethics is about good practice when collecting, using and sharing data. Data ethics is particularly relevant when the processing of data can affect people and society, directly or indirectly. The focus of data ethics is therefore not on data as such, but rather on the human actions that relate to data.

Data processing must take place within the framework of legislation, but data ethics is not law. Data ethics is about more than complying with the formal rules that already apply in data protection.

A problem is not data ethical only because it concerns the processing of data. The data processing must also raise an ethical dilemma. A data ethics dilemma arises if the use of data conflicts with one or more of our central values or principles. As appears below, our primary data processing takes place in accordance with established agreements and specific instructions from our customers to support them in their fulfilment of legal and contractual obligations. The aforementioned dilemmas will therefore primarily arise in situations where we are the data controller as defined in the GDPR.

All choices have consequences and the positive considerations must outweigh the negative ones. We must find a reasonable balance between, on the one hand, the many advantages that the use of data and new technology provides, and on the other hand, the consequences that the use of data can have for the individual person and for society, both in the short and long term. Making informed decisions is thus a central part of data ethics.

To act in an informed and ethical way, we must first determine the basic values on which our processing of data is based. Next, these values must be communicated to all employees in a way that makes the values understandable and natural to observe.

It is necessary that our employees are informed and understand the guiding principles governing how we, as an organisation, collect, use and share data in a way that we can vouch for as ethically sound.

With this aim we have formulated our Data Ethics Policy, which serves as a guideline on how we process data. The Policy applies to all data processed by us and all employees are expected to comply with this Policy.

Our Data Ethics Principles

In Visma, our position towards data ethics is based on three principles that underlie our values. Defining distinct data ethics principles ensures alignment across our organisation and sends a strong signal to our customers and business partners. We place a decisive emphasis on communicating our principles to all employees working with data.

Both in relation to the data processing we carry out on behalf of our customers, and in relation to the data processing we carry out for our own purposes, the following principles apply:

Transparency

The landscape of payroll processing is fraught with challenges, from compliance issues to the complexities of managing a workforce. Our use of data must therefore support a culture, where automation and simplicity enhance our end-customers' payroll accuracy and reduce their costs associated with errors and improve their overall operational efficiency.

It is therefore crucial that our processing of data is sufficiently transparent. This implies that the customer must have access to insight into their own data, and that all information about the processing of data - purpose, functions, security, limitations etc. - must be given clearly and comprehensibly. The underlying patterns must be explainable and justified.

The received data must be processed exclusively in accordance with the agreement, applicable legislation and solely to fulfil the obligations under the agreement.

We must provide each customer online access to the data we have registered or created for the customer via our data processing. Furthermore, we must inform the customer about the progress of specific cases we process for the customer.

Security

Processing of data must be sufficiently secure, robust and reliable. Content and scope of data should be limited as much as possible and data must not be stored for longer than absolutely

necessary. Sharing may only take place within the framework permitted by legislation and agreements.

There must be security around the storage and sharing of data, so that data does not inadvertently become available to unauthorised persons. Only employees with a work-related need to access data are granted access, and access restrictions must be updated when needed.

It must be possible to monitor and exercise effective supervision and control so that errors and potential negative social or ethical consequences can be identified, evaluated, documented and minimised.

Accountability

In relation to customers we ensure that the individual customer is aware of our responsibility, including the limitations of our liability. We treat the trusted data responsibly, and we inform the customer if we due to special circumstances, e.g. specific legal obligations, have to deviate from the concluded agreement and the customer's instructions.

Internally, between the various departments, and in relation to business partners and third parties, it must be clear at all stages who is responsible for the consequences for the development and use of data. This applies, among other things, to developers and users.

When personal data is anonymised, we ensure that no natural persons can be identified based on the information or in combination with other information, and that the information cannot be traced back to an identifiable or identified natural person. The anonymisation is irrevocable.

Our processing of data

Processing of data inside our products

Our core service is to provide systems and associated services where business customers themselves register information about their employees for use in payroll processing. In addition we offer add-on products for use in personnel administration and time registration.

By far the largest amount of data we process relates to our core services. This processing takes place on behalf of and based on instructions from customers, and in order for us to administer the contractual relationship. When processing data in relation to these services we collect and process data in accordance with the agreement with our customers, defined processing rules, specific instructions and the relevant legislation.

The sections below explain the different categories of data that we process, including how we collect the data of our customers. To provide clarification, when referring to customers, we

include all companies and individuals that we interact with to provide our application and other services, including website visitors, potential leads, and end users of our applications.

Customer data collected through our applications

In order to use our products, our customers share their data regarding the customer himself (the company) and personal data concerning the customer's employees - all within the areas of payroll administration, personnel administration and time registration.

Each individual customer has full control over which data we process. The customer selects which data to upload to our applications and which integrations to enable in order for data to flow through their systems into ours by our open APIs. Correspondingly, the customer decides the exchange of data from our applications to the customer's own. To ensure transparency, we do our best to make it clear exactly which data will be exchanged between the applications.

We collect anonymized data about the customers' use of our products. We are committed to use this data only to improve, optimise and develop our products and services and thereby generate more value for our customers.

Our data processing agreements with customers allow us to anonymise and aggregate the customers' data and their use of our products. We use these data to prepare statistics on wage formation and wage development, company and employee circumstances and demographics.

Company data collected from public authority's registers

On behalf of the individual customer we collect the name and address of employees that the customer creates in the payroll system from the Danish CPR register (containing all persons registered with a Danish ID).

Furthermore, we collect data from the Danish Customs and Tax Administration to be used for our customers' withhold of tax and labour market contribution on the salary of their employees. When a customer registers an employee, we create a subscription to the employee's "tax card". The subscription ends when the employee resigns or if the company ceases to be a customer.

Customer support data

When providing support to our customers, data is collected through our chat, email and phone systems.

As part of our chat, we have developed an AI powered tool that both Customer Success consultants and customers can use. It provides answers from our knowledge base and systems. The tool is described further under the section "Use of new technologies" below.

We record and store phone conversations with customers in order to document what was said during the conversation, including any agreements made. The conversations are saved for 90 days, after which they are automatically deleted.

We continuously send out customer satisfaction surveys and market surveys where we gather customer feedback.

Processing of data outside our products

Our processing of data must take place with respect for privacy and the protection of personal information. Consideration should always be given to what data is needed, from which sources data is to be obtained and how sensitive this data is considered to be.

In relation to the data processing for which we ourselves are responsible, i.e. in relation to contract administration, processing of customer data for our own purposes and processing of data concerning our own employees, privacy is a purpose that we must ensure compliance with.

Employee data

Visma DataLøn og ProLøn A/S' own data, including data on our own employees, are processed in accordance with the data protection rules. Our employees are informed of the processing and data is used solely for the purpose for which they are collected, namely to manage all aspects of the employment relationship from employment to termination.

In addition, data on own employees is used to a limited extent for data analysis purposes such as analyses and trends etc., about absence, staff turnover etc.

Data collected on our website and from Social Media

Ethical considerations in connection with our profiling and our collection of data must also include the nature of our products. We are primarily a payroll service provider, and the products and services we market are aimed at companies - not persons. Therefore, the non-sensitive data we collect via these channels is linked to business activity and not to purely personal matters.

The performance data we collect from Social Media is anonymous. The collection takes place in order to gain general knowledge about reactions, etc. on our ads. Only when a user visits one of our websites and accepts cookies do we identify the visitor and collect additional agreed information.

Our cookie declaration presents our cookies in an open and transparent manner in order to make it clear how cookies are used so that the visitor can make an informed choice about allowing or rejecting their use. A cookie consent can always be withdrawn, and upon request we provide all data we have recorded about a user or potential customer.

We collect data about the user to monitor how our website is used in order to make our online services easier to use, create a good user experience and present the most relevant content. The information helps us deliver the best service and adapt the software to the needs of our customers. Data is also collected for the purposes of marketing, including identifying leads.

We use an AI powered support tool for our website to answer customer queries instantly in a user-friendly interface.

Any personal data collected through our website is governed by our Privacy Policy, which customers are able to access at all points of the data collection on our website.

Data collected for the provision of legal assistance to customers

We offer general and specific telephone and/or written legal advice in relation to personnel administration and employment law. When specific tasks are to be solved, an agreement on the task is entered into with the customer to align expectations etc. The customer supplies the data and information, including personal data, that is agreed and necessary for our task solution.

A main focus for us is to ensure that complex law regulation within employment law is communicated through simple and clear communication which ease handling of personnel administration.

We only advise within our legal core expertise. It is essential for us to act as a trusted advisor to ensure long term customer relationships.

Sharing of non-application data

We share data with trusted third parties for them to process data based on our instructions and defined purposes of providing our products and services to our customers as well as carrying out marketing activities towards potential customers.

The sharing of data is helping us to deliver customer support, manage customer contacts, improve our processes through gathering feedback, and analyse customer behaviour. Sharing data in this case is done on agreed terms and in compliance with our Privacy Policy. We have an internal procedure in place to ensure that vendors who we share data with are approved in relation to their level of compliance to the GDPR and implemented security practices.

Sharing data when required by law

In some cases, we are obliged to share data with public authorities or curators. Before sharing any data, we make sure that there is a legal authority or a legitimate court order in place. Furthermore, we ensure that the request contains a precise delimitation of the requested information in relation to data subjects, types of information, period etc.

We inform the affected customer about the delivery, unless the requisition contains a reasonably justified request that this should not take place. In this way, we generally ensure that the data controller is fully informed and can follow the process.

Use of data to track atypical or illegal behaviour

We monitor the dark web in order to identify passwords, etc., intended for use in our products, but which are now offered so that others may gain unauthorised access.

Furthermore, on the basis of inquiries from customers or authorities, we monitor registrations and transactions in the event of justified and specific suspicion. In doing so, we try to help prevent, among other things, misuse of personal data to obtain unjustified financial gain. Such cases are treated separately and carefully and in strict compliance with the GDPR, including in relation to the processing authority and our access to disclose information.

Use of new technologies

At Visma DataLøn and ProLøn A/S, we use algorithms, machine learning, and artificial intelligence (AI) to enhance our products and create value for our customers. However, we recognize that leveraging new technologies requires a commitment to ethical and responsible practices.

Over many years, we have validated the data we receive from our customers, to ensure that the data meets the form requirements etc. that apply to reporting the relevant type of data. These checks are continuously improved with a view to catching input errors etc., so that data is as correct as possible when submitted for processing. The technologies make it possible also to carry out reasonableness and probability checks, etc., e.g. in relation to report type and/or the individual customer's previous input.

By using these technologies we can also obtain additional knowledge and gain better insights into the data the customers process, which in turn can be the basis for business and product decisions and improve the products and services offered to customers.

Our AI models does not process sensitive data, and as a B2B company, our models pose small risks to our customers' fundamental rights. Personal data about customers´ employees can be processed by AI when it is provided to us by the customer through our systems. However, AI will never make decisions regarding the employment relationship, but advise on legislation and processes in our systems. By ensuring that the customer has the final say, we try to minimize the impact of our AI on the employees rights.

When our customers interact with our AI they are informed in a transparent way, about responsible use. They are informed that the AI does not make decisions, but presents information to help the customer make informed decisions. The AI is trained on internal data, thereby the risk of infringement of third party risks are minimized.

To uphold ethical standards, we have established clear guidelines for employees working with AI. These include working to eliminate bias by monitoring results for objectivity and fairness, and continually improving our models to ensure accuracy and transparency.

By integrating new technologies responsibly, we aim to enhance customer experiences and support their workflows, all while safeguarding privacy and maintaining our ethical obligations.

Anchoring of our Data Ethics Policy

We believe that having strong data ethics is vital and since we want to maintain and develop our ethical culture and continue to have our customers' trust, it’s essential to involve the whole organisation.

It has been decided to anchor our policy for data ethics in our Information Security Board, which consists of members of the top management, legal and security.

The board meets monthly and reviews policies and risks concerning regulatory compliance, security and data ethics.

Any questions which are not being answered through these guidelines can be directed to our managing director, Jesper Lundgreen.

Review and approval of this Policy

The Information Security Board is overall responsible for our compliance with this Policy. The Policy will be reviewed and approved at least once annually, and the current version is available to employees at all times and on our website. The policy forms the basis for the data ethics report in connection with the management report.