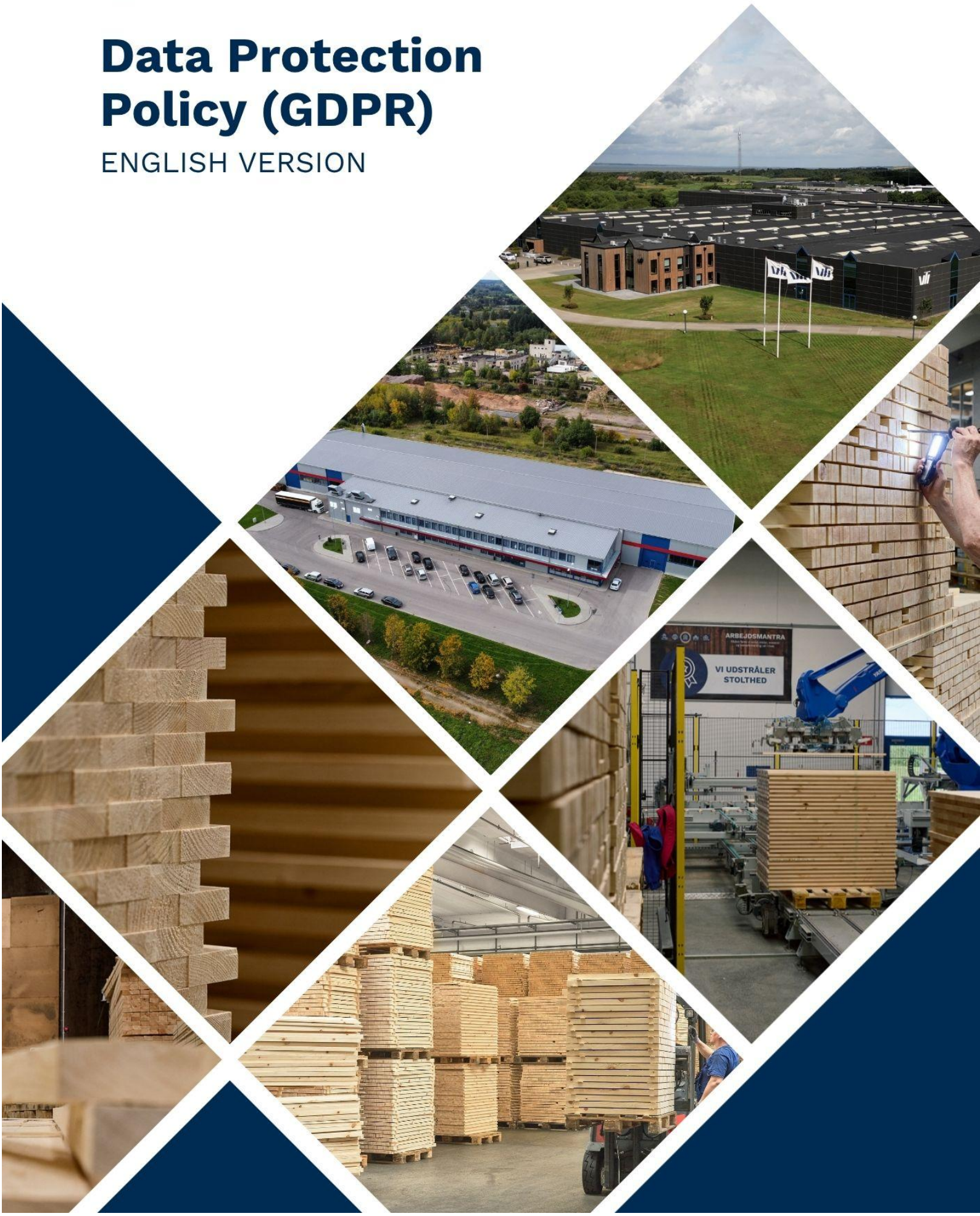
Data Protection Policy (GDPR)

ENGLISH VERSION



PURPOSE

The purpose of this policy is to establish and describe the company's rules on the protection of natural persons (the data subjects) in connection with the processing of personal data in the company.

BACKGROUND

This policy is based on Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR"), as well as applicable national laws and guidelines.

The Company is a data controller and strives to maintain and continue to build a strong data protection and privacy culture to protect all the personal data collected and processed within the Company.

The processing of personal data is generally related to the company's own employees, but also deals with the processing of personal data related to the company's business activities. This policy thus describes the rules and guidelines that the company has determined must be used when processing personal data for its own employees and other relevant data subjects.

In order to adequately protect the personal data, the company continuously assesses the level of risk associated with the data processing. The company is particularly aware of the risks of discrimination, ID theft, financial loss, loss of reputation and data confidentiality.

LIABILITY & APPLICATION

This policy replaces previous data protection policies and applies to all data subjects in the company, including employees. The policy is used for the processing of personal data that is wholly or partly carried out by means of automated data processing, and for other non-automated processing of personal data.

DEFINITIONS & EXPLANATIONS

"Processing" means any operation or set of operations, whether or not by automated means, which is performed on personal data or on a set of personal data, such as collection, recording, organisation, organisation, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other form of disclosure, alignment or combination, restriction, erasure or destruction;

"biometric data" is to be understood as personal data which, as a result of specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, enables or confirms the unambiguous identification of that person, such as facial image or fingerprint data;

"Personal Data Breach" is to be understood as a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

"Data controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means for which personal data may be processed

"Processor" means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the Controller;

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data

"Genetic data" is to be understood as personal data relating to the inherited or acquired genetic characteristics of a natural person, which provide unambiguous information on the physiology or health of that natural person, and which are obtained, in particular, following an analysis of a biological sample from that natural person

"Health data" is to be understood as personal data relating to the physical or mental health of a natural person, including the provision of health services, and which provides information on his or her state of health;

"Personal data" means any information relating to an identified or identifiable natural person ('data subject'); An identifiable natural person means a natural person who can be identified, directly or indirectly, in particular by means of an identifier such as a name, an identification number, location data, an online identifier or to one or more elements specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"Data subject's consent" is to be understood as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which the data subject consents, by declaration or clear affirmation, to the processing of personal data relating to him or her

"the company" is to be understood as VTI Vinderup Træindustri A/S

PRIVACY POLICY

DATA PROTECTION AND PRIVACY PRINCIPLES

The protection of personal data is of great importance to the company. This applies both in relation to its own employees, to customers and suppliers as well as other data subjects where the company processes personal data.

This policy has been adopted to:

- comply with applicable laws and practices;
- protect the employee's personal data
- protect the personal data of other data subjects;
- Protect your company's data
- process personal data that is necessary to fulfil the company's obligations as a data controller;
- minimize the use of consent to only those situations where no other legal method/legal basis exists to process personal data;

Data protection is the responsibility of all employees. It is very easy to unintentionally disclose information about a colleague to a customer or a friend, or about a customer to a spouse or relative. To avoid this, all employees should avoid discussing matters that could potentially lead to non-compliance with this policy.

The company basically wants to protect the privacy and confidentiality of natural persons. The Company acknowledges that not only its own employees, but also customers, suppliers and other data subjects with whom the Company comes into contact during a working day, are entitled to know that their respective personal data will not be used for any purpose other than the original one.

In order to comply with applicable laws and practices, personal data will be collected and processed according to the purpose, as well as stored securely and not disclosed to other persons/third parties without the consent of the data subject.

PRINCIPLES FOR PROCESSING PERSONAL DATA

Personal data in the company must:

- lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- collected for explicitly stated and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes ('purpose limitation');
- be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- be accurate and, where necessary, up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate in relation to the purposes for which they are processed are promptly erased or rectified ('accuracy');

- be retained in such a way that it is not possible to identify the data subjects for a longer period than is necessary for the purposes for which the personal data in question are processed ('retention restriction');
- processed in a manner that ensures adequate security of the personal data concerned, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality');

PROCESSING OF SENSITIVE PERSONAL DATA

The GDPR defines an exhaustive list of sensitive personal data that the company does not process, unless there is a clear legal basis, a labour law obligation or unambiguous consent:

- racial or ethnic origin
- political, religious, or philosophical beliefs
- trade union affiliation;
- genetic data, biometric data
- Health Information
- sexual relations or sexual orientation

If the company processes one or more sensitive personal data, this data will be deleted after use/at the end of 6 years from the date on which the company received the sensitive personal data in question.

Sensitive personal data is not transferred to countries outside the EU/EEA area unless there is a clear legal basis and an adequate level of protection of the data subject's sensitive personal data in the country in question.
Attached as Appendix 1 to this policy is a list of the sensitive personal data that the company collects and processes, including the purpose and basis for processing. The list is updated regularly.

TREATMENT ACTIVITIES

The Company processes personal data about its employees, especially in relation to the employment relationship, but also about the Company's suppliers, partners and other third parties (other data subjects).
Processing of personal data in the company is generally (i) necessary according to a contract to which the data subject is a party, (ii) necessary to comply with a legal obligation, or (iii) based on a written consent from the data subject who consents to the company e.g. processing personal data before, during and after the employment relationship.
In order to document the company's various data flows, the company has described and documented all relevant processes where personal data is collected and processed. These process descriptions constitute an appendix to this policy and are attached as Appendix 2.

PURPOSE OF PROCESSING PERSONAL DATA

The Company collects, processes and stores the personal data of the data subjects in connection with certain lawful, including business, purposes. This happens, for example, when the company needs to:

Use employee information:

- Name
- Contact information, including residential address
- CPR no.
- Images
- Employment
- Salary conditions
- Education
- Work experience
- Bank & pension information
- Sick leave
- Personality test, IQ test, business test
- Etc.

It may be necessary for the company to process the following sensitive personal data both during employment and at the end of employment:

Information about criminal offences

- Significant social problems
- Health Information
- Information about the reason for dismissal or expulsion
- Etc.

Use customer information:

- to provide customers with the services they have requested;
- for invoicing and accounting purposes
- to enable the company to respond to customer inquiries
- for verification of customer identity (security purposes);
- to market the company's services and products to customers;
- Etc.

use business-related information:

- to maintain company financial statements and business documents;
- to allow the company to respond to inquiries
- to verify identities
- Etc.

Use domain names and email addresses:

- in such a way that cannot be referred to a particular individual. This is done with a view to:

- on quality control and improvement of the company's website
- to send news about the services that visitors to the website have signed up for;
- to inform customers about other services of the company;
- Etc.

use financial information, including credit card information:
This information is used for the purpose of getting payment for goods and services. The company does not store this information for longer than is necessary to carry out a processing.

If the company wishes to use the data subjects' personal data for a purpose other than the original one, the data subject will be informed of the new purpose and request the data subject's consent before the data processing begins. If there is another legal basis for the new processing, this will inform the data subject.

The company wants to be sure that only personal data that is necessary for the specific purposes is processed. The company's IT systems are therefore designed so that only the necessary amount of data is collected and the personal data is not stored for longer than necessary.

CONTROL MEASURES
The Company continuously checks and updates the collected personal data to ensure that the personal data processed about the data subjects is not incorrect or misleading.

As the Company's administration is dependent on the employee's personal data being correct and up-to-date, the Company requests the employees to inform about relevant changes to the personal data. In this connection, the employee must contact
payroll accounting.

RIGHTS OF THE DATA SUBJECT
The Company, as the Data Controller, shall take appropriate measures to provide any information concerning processing to the Data Subject in a concise, transparent, easily understandable and easily accessible form and in clear and simple language. The information is provided at the request of the data subject in a written or electronic form.

If personal data about a data subject is collected from the data subject, the company, as data controller, at the time the personal data is collected, provides the data subject with all of the following information:
- the identity and contact details of the controller and, if applicable, its representative;
- the purposes of the processing for which the personal data are to be used and the legal basis for the processing;
- the legitimate interests pursued by the controller or a third party;
- any recipients or categories of recipients of the personal data;
- where applicable, the controller's intention to transfer personal data to a third country;

In addition to the above information, the Company, as the Data Controller, at the time the Personal Data is collected, provides the Data Subject with the following additional information necessary to ensure fair and transparent processing:

- the period during which the personal data will be stored or, if this is not possible, the criteria used to determine this period
- the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing, as well as the right to data portability;
- the right to withdraw consent at any time, without prejudice to the lawfulness of processing based on consent, before its withdrawal;
- the right to lodge a complaint with the Danish Data Protection Agency
- whether the provision of personal data is mandatory or a requirement under a contract or a requirement that must be fulfilled in order to enter into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of not providing such information
- the existence of automated decision-making, including profiling, and at least meaningful information about the logic thereof and the significance and expected consequences of such processing for the data subject.

If the personal data has not been collected from the data subject, the company, as data controller, provides the data subject with the following information:

- the identity and contact details of the controller and, if applicable, its representative;
- the purposes of the processing for which the personal data are to be used and the legal basis for the processing;
- the categories of personal data concerned
- any recipients or categories of recipients of the personal data;
- where applicable, the controller's intention to transfer personal data to a recipient in a third country;

In addition to the above information, the Company, as the Data Controller, provides the Data Subject with the following information necessary to ensure fair and transparent processing with respect to the Data Subject:

- the period during which the personal data will be stored or, if this is not possible, the criteria used to determine this period
- the legitimate interests pursued by the controller or a third party;
- the right to request from the controller access to, rectification or erasure, of personal data or restriction of processing concerning the data subject and to object to processing, as well as the right to data portability;
- the right to withdraw consent at any time, without prejudice to the lawfulness of processing based on consent, before its withdrawal;
- the right to lodge a complaint with the Danish Data Protection Agency
- the source of the personal data and, if so, whether it originates from publicly available sources;

- the existence of automated decision-making, including profiling, and at least meaningful information about the logic thereof and the significance and expected consequences of such processing for the data subject.

The company provides the information listed above:

- within a reasonable period of time after the collection of the personal data, but no later than within one month, taking into account the specific circumstances under which the personal data have been processed;

The data subject's right of access
The data subject has the right to obtain the company's confirmation as to whether personal data concerning him or her is being processed and, if so, access to the personal data and the following information:

- the purposes of the processing
- the categories of personal data concerned
- the recipients or categories of recipients to whom the personal data are or will be disclosed, if possible, for the envisaged period of time for which the personal data will be stored;
- the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject, or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- any available information on the origin of the personal data if it is not collected from the data subject;
- the existence of automated decision-making, including profiling, and at least meaningful information about the logic thereof and the significance and expected consequences of such processing for the data subject;

RIGHT TO RECTIFICATION
The data subject has the right to have incorrect personal data about him or her corrected by the company without undue delay. Taking into account the purposes of the processing, the data subject has the right to have incomplete personal data completed, including by submitting a supplementary statement.

RIGHT TO ERASURE ('RIGHT TO BE FORGOTTEN')
The data subject has the right to have personal data about him or her deleted by the company without undue delay, and the company is obliged to delete personal data without undue delay if one of the following circumstances applies:

- The personal data is no longer necessary to fulfil the purposes for which it was collected or otherwise processed
- The data subject withdraws his or her consent and there is no other legal basis for the processing

- The data subject objects to the processing and there are no legitimate grounds for the processing that precede the objection
- The personal data has been unlawfully processed
- The personal data must be erased in order to comply with a legal obligation under EU or Member State law to which the company is subject.

RIGHT TO RESTRICTION OF PROCESSING

The data subject has the right to obtain restriction of processing from the company if one of the following circumstances applies:

- The accuracy of the personal data is disputed by the data subject, in the period until the company has had the opportunity to determine whether the personal data is correct
- the processing is unlawful and the data subject opposes the erasure of the personal data and instead requests that its use be restricted
- the controller no longer needs the personal data for the processing, but it is necessary for the establishment, exercise or defence of a legal claim
- the data subject has objected to the processing during the period while it is checked whether the legitimate interests of the company take precedence over the legitimate interests of the data subject

Duty to notify in connection with rectification or deletion of personal data, or
Restriction of processing

The Company shall notify each recipient to whom the Personal Data has been disclosed of any rectification or erasure of the Personal Data or restriction of processing;
unless this proves impossible or is disproportionately difficult. The company will inform the data subject about these recipients if the data subject so requests.

RIGHT TO DATA PORTABILITY

The data subject has the right to receive, in a structured, commonly used and machine-readable format, personal data concerning him/herself that he or she has provided to a controller and has the right to transmit this information to another controller without hindrance from the controller to whom the personal data have been provided, where the processing is based on consent or on a contract and the processing is carried out by automated means.
Right to object and withdraw consent

The data subject may at any time object to the processing of the data subject's personal data and thereby withdraw a previously given consent to the processing.

However, the data subject must be aware that any revocation may be contrary to the company's essential interests, and that the revocation may have consequences, for example, for an employee's employment conditions. Furthermore, there will be certain personal data that the company will be able to process without the data subject's consent, if the company has a legitimate interest in the processing and that the consideration for the data subject does not exceed this interest.

Automated individual decision-making, including profiling
The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which has legal effects or similarly significantly affects him/her.

DATA PROCESSORS
As part of the Company's processing of personal data, the Company is from time to time obliged to transfer personal data to third parties.

Transfers to third parties include, but are not limited to:

- KMD/E-Boxing
- National Board of Industrial Injuries
- TAX
- Pension & Insurance Providers
- Public authorities to which the company is required by law to disclose personal data about its employees.

The company has entered into data processing agreements with all its data processors, and has these agreements registered in its systems.
Education and training
Training and education on the GDPR, including local laws and practices, as well as this policy, is regularly offered to the company's employees.
Specialist training in relation to GDPR is offered as needed to specific groups of employees who work with and are responsible for the company's data protection on a daily basis, including responsibility for this policy and attached process descriptions, etc.

DATA SECURITY
The company has decided not to hire an internal or use an external data protection officer (DPO) as defined in the GDPR.
Instead, the company's board of directors has decided and approved the establishment of a 'Data Protection Network', which must consist of at least 1 representative from the management who is the company's IT manager and 1 employee representative. The 'Data Protection Network' is responsible for the day-to-day management of the company's data protection, including implementing and ensuring appropriate GDPR compliance within the company.

The Company ensures that personal data is always kept safe from unauthorized or unlawful loss or disclosure. In addition, the company has a backup procedure for all its personal data. The employee responsible for the company's IT infrastructure is responsible for specific and detailed IT security policies that regulate the security elements of the GDPR on behalf of the company.

VIOLATIONS AND SANCTIONS
Any violation of this policy must be reported to the company's IT manager in his capacity as chairman of the company's 'Data Protection Network'

If an employee unauthorisedly discloses the company's personal data to a third party, such an action may have employment law consequences for the employee in question.

REPORTING
The Chairman of the Company's 'Data Protection Network' reports to the Company's Board of Directors once a year with regard to the status and level of GDPR Risk and Compliance in the Company.

APPROVAL – AMENDMENTS AND ADDITIONS
This policy is approved by the company's president/CEO.

Changes to or additions to this policy must be made by the Chairman of the Company's 'Data Protection Network', and finally approved by the Company's President/CEO.