Privacy Policy in Dynea AS

Author:	*Ann-Magrit Nome Sommervold*	Revision number:	*3*
Revised date:	*12. Oct. 2023*	Quality number:	*1001764*
Approved by:	*Stefan Olsson*	Next revision:	*12. Oct. 2025*

General provisions on the processing of personal data in Dynea

1. Purpose

These guidelines, valid and frame at the same time for Dynea AS and its subsidiary, hereafter Dynea, or the Company, aim to ensure that the processing of personal data in Dynea is conducted in a manner that complies with the current data protection legislation and any agreements made with Dynea's employees, job applicants, customers, suppliers, partners, potential customers or other business contacts.

When in doubt on how to process personal data, please contact a superior responsible for either the processing of personal data or security.

1.1 Contact Persons

Contact persons		
Role	Holder	Responsibilities and contact details
Data Protection Officer	Ann-Magrit Nome Sommervold	Is responsible for the implementation of the adequate security measures to ensure the protection of personal data. Email: ann.sommervold@dynea.com Phone: 951 46 741
Security Officer for Data Protection	Bjørn Rosbach	Assists the Data Protection Officer in the implementation of adequate security measures to ensure the protection of personal data. Email: bjorn.rosbach@dynea.com Phone: 90049980

Dynea has assessed whether it must appoint a data protection officer in accordance with the requirements in the Act relating to the processing of personal data (the "**Personal Data Act**") and articles 37 to 39 of GDPR, finding that the requirements are not fulfilled. Hence, the Data Protection Officer named in the table above shall not be deemed as a data protection officer in the meaning of the Personal Data Act and articles 37 to 39 of the GDPR.

1.2 Personal Data – Definitions

Personal Data is any information related to a person that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address. Personal Data does not include anonymous or non-personal information (i.e., information that cannot be associated with or tracked back to a specific individual).

2. General Overview – Dynea's Processing of Personal Data

2.1 Summary

Dynea processes personal data of employees, job applicants and contact persons associated with employees, customers, suppliers, partners, potential customers and other business associates (hereafter collectively "Business contacts").

Dynea processes such personal data as a data controller (that is, deciding the purpose of the processing of personal data).

The main purpose of this processing of personal data will normally be to fulfil the Company's obligations towards employees, job applicants and Business contacts, and to offer them our services in the best possible manner.

The Company does at the moment not process any information from Business contacts for marketing purposes.

The personal employee data processed consists mainly of general personal data, such as name, national ID no, address, email-address, phone number, nearest relatives, CV, competence, employment contract, non-disclosure agreements, employee reference letters etc. Moreover, Dynea also processes some sensitive information on employees, including health information to fulfil the requirements set forward in the Norwegian regulation concerning the performance of work (NW: "*Forskrift om utførelse av arbeid*") (the "Regulation"). The Regulation requires the Company to process and store the individual employee's name, national ID number, position and workplace, as well as information regarding which hazardous chemicals the employee is exposed to. The information shall be stored for 60 years.

In our view, the processing of personal data in accordance with the requirements set forward in the Regulation and has a valid legal basis. The purpose of the regulation is to make sure that Dynea has an overview of which hazardous chemicals the employees has been exposed to. Some of the chemicals the employees are exposed could possibly be carcinogenic. Thus, the processing and storage of personal data complies with the requirements of GDPR, as the processing is both necessary to comply with a legal obligation and serves a legitimate interest. The way we see it, the Regulation shall be deemed as *lex specialis* contra GDPR in this manner.

2.2 Fundamental principles of the processing of personal data

The Personal Data Act establishes certain fundamental principles for the processing of personal data, which apply to all our processing of personal data.

These fundamental principles constitute independent obligations under the regulations, and the breach of the obligations may in itself represent breaches of law and may result in the imposing of fees. Dynea must always observe the principles listed below during the processing of personal data:

- *Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*
- *Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');*
- *Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*
- *Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that if personal data are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');*

- *Personal data shall be kept in a form which permits identification of data subjects for no longer than what is necessary in relation to the purpose of the processing ('storage limitation');*

- *Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*

The Security Officer for Data Protection shall always be contacted in the event of any request from external parties concerning data protection, including any requests from the Norwegian Data Protection Authority.

2.3 The legal basis for our processing of personal data

All processing of personal data must have a legal basis in the Personal Data Act.

The overview below presents the various legal bases for the legal processing of personal data and is based on GDPR Article 6 (1). The most relevant basis for our activities has been highlighted in bold font:
The data subject has given consent to the processing of his or her personal data for one or more specific purposes;

a. **Processing is necessary for the performance of a contract to which the data subject is party** or in order to take steps at the request of the data subject prior to entering into a contract;
b. **Processing is necessary for compliance with a legal obligation to which the controller is subject;**
c. Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
d. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
e. **Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Most of Dynea's processing of personal data is necessary for the performance of a contract to which the data subject is a party or to comply with a legal obligation to which Dynea is a party. Such data shall not be processed beyond that there is legal basis for in the Personal Data Act. If no other legal basis is applicable, Dynea will mostly base its processing of personal data on consent. Such processing shall meet the requirements for consent in the Personal Data Act, and the processing of personal data shall not go beyond what is covered by the consent, nor be processed for new purposes.

The legal basis for and the purpose of the processing of personal data of employees and job applicants and Business contacts is further described in Section 2.4 to 2.7 below

2.4 Processing of personal data of employees

Dynea act as a data controller when it comes to the processing of personal data of employees. Dynea's processing of personal data of their employees consist of the processing of contact details and HR-information, such as name, social security number, address, phone number, e-mail, photo, nearest relative, CV, competence map, employment contract, non-disclosure agreements and employee reference letter ("Employee data").

Moreover, according to the Regulation mentioned above in 2.1, Dynea is required to process data regarding which hazardous chemicals the employee is exposed to.

The purpose of Dynea's processing of personal data of employees is mainly to enable payment of wages to the employees, register employees in mandatory insurance arrangements, payment of pension contribution.

Dynea employees general contact data, such as name, e-mail address, photo and phone number(s) are used in communication within the company (i.e., on intra and sending e-mail), and for physical access to the company and the company's IT systems.

Dynea will never post pictures or other personal data of an employee on social networks or externally without specific consent.

The legal basis of Dynea's processing of personal data of employees is based on either GDPR art. 6 (1) a (consent), GDPR art. 6 (1) b (contract) or GDPR art. 6 (1) c (legal obligation). The legal basis for Dynea's limited processing of health information on the employees, in accordance with the provisions in the Regulation, is GDPR art. 9 (2) b (compliance with a legal obligation in the field of employment and social security and protection law).

Dynea's routines for storage and deletion of personal data is set out in Section 6.

2.5 Processing of personal data of job applicants

Dynea act as controller when it comes to the processing of personal data of job applicants. Dynea's processing of personal data of job applicants consist in the processing of contact details, birth date as well as other information provided in the CV or the job application.

The purpose of Dynea's processing of personal data of job applicants is the administration of these applicants in the Company's internal registers and securing the authentity of the applicant.

The legal basis for Dynea's processing of the personal data of the possible customer is GDPR Art. 6 (1) a (consent).

Dynea's routines for storage and deletion of personal data are set out in Section 6.

2.6 Processing of personal data of Business contacts

Dynea act as data controller when it comes to the processing of personal data of contact persons from Business contacts. In this regard, Dynea processes name, and contact info of the relevant contact persons.

The purpose of Dynea's processing of personal data of Business contacts is to be able to enter into and maintain customer-, partner- and supplier contracts, to carry out the services as provided in the contracts, as well as conducting further development of products and services. Activities such as collecting and processing data prior to providing an offer, maintaining and promoting contact with Business contacts, handle orders and recalls, provide customer service, performing analysis of market surveys and marketing strategies in turn to perform adequate further development of products and services may use contact information. This processing is necessary to fulfil our contractual obligations and be a partner in developing the business further, follow-up and support of previous contracts and moreover serves a legitimate purpose.

The legal basis of Dynea's processing of personal data is either GDPR art. 6 (1) b (agreement) or art. 6 (1) f (legitimate interest).

Dynea's routines for storage and deletion of personal data are set out in Section 6.

2.7 Marketing

Our marketing is mostly general and does not involve any processing of personal data. However, in connection with fairs we sometimes collect personal data on potential customers' contact person in order to follow up the initial interest. If the initial interest disappears, our marketing ceases.

The processing of personal data will happen in connection with collecting, checking and processing data prior to providing an offer. This processing of data will be based on consent and moreover serves a legitimate purpose. Thus, the processing of data has its legal basis in GDPR article 6 no. 1 (a) or (f).

2.8 Cookies

Dynea act as data controller when it comes to processing of personal data collected through cookies in the Dynoadd website. The purpose of Dynea's use of cookies is to be able to ship samples. We do not collect cookies on our Dynea.com website.

The legal basis of Dynea's processing of Dynoadd website-visitors' personal data is GDPR Art. 6 (1) a (consent).

3. Where personal data is processed

The data protection regulations set out conditions for the processing of personal data depending on where the personal data is being processed.

Dynea may use third parties in regard to their processing of employee data, i.e., auditors, legal advisors, IT-service providers and travel agencies. Personal data of employees may therefore be transferred to the processors available on L:\HR\GDPR folder.

Personal data of the customers, suppliers and partners may also be disclosed to Dynea's auditors, legal advisors and IT-service providers. The personal data shared with Dynea's auditors and legal advisors will in no circumstances be stored or processed outside of the EEA without explicit agreements.

See also Section 5 below concerning the processing of personal data by third parties on behalf of Dynea.

4. Who is processing personal data internally in Dynea

Processing of Employee personal data internally in Dynea beyond name, e-mail address, photo and phone no is handled with restricted access. When it comes to processing of other personal data of the employees, including health information, only the closest superior, as well as the HR-manager, HSE representative and administrative secretary, will have access to the relevant information. The restricted access applies to, i.e., the data in our HR system and to the physical records in the HR archive. These records shall not move out of the archive room.

Dynea may however give other employees than those mentioned above access to the relevant information if it is necessary to fulfil their responsibilities, i.e., in connection with recruitment processes and payment of salary.

When it comes to internal processing of personal data of customers, suppliers and partners, Dynea may give employees access to this information if they are involved in the services provided to the customer, supplier or partner, and this is necessary to carry out their obligations to the relevant contracting party.

5. Processing of personal data by third parties on behalf of Dynea

Dynea acts as a data controller in relation to the processing of personal data of its employees, job applicants and Business contacts cf. the definition of the 'controller' and 'processor' in the Personal Data Act. This means that Dynea has the overall responsibility for the processing of personal data.

If third parties process personal data on behalf of Dynea, they are to be considered as processors, cf. the definition of processors in the Personal Data Act.

There shall always be a data processing agreement between Dynea and the processor, and the processor shall not process personal data beyond what follows from this agreement. The agreement must comply with the data protection legislation.

Certain companies have generic data processing agreements, limiting their area of operation and describing their procedures, i.e., several IT service providers.

Personal data shall not be transferred to third countries, i.e., mainly, countries outside the EEA, unless there is a specific legal basis for such transfer (e.g. through an agreement based on the EU's Standard Contractual Clauses, or any other scheme approved by the EU).

An overview of Dynea's processes are available from our systems overview on Sharepoint, IT landing pages.

6. Storage and deletion of personal data

6.1 General procedures

Personal data shall not be stored for longer than what is necessary to achieve the purpose of the processing of the personal data. In addition, certain statutory requirements apply to the storage of data, both in the accounting legislation and in health regulatory regulations.

6.2 Special procedures for storing and deleting personal data of employees and job applicants

All personal data regarding Dynea's employees, except contracts of employment, non-disclosure agreements, employee reference letter and new email address, will be de deleted upon termination of employment managed via an off-boarding process. The same goes for job applicants.

The only exception from this main rule, is the Regulation mentioned in 2.1, committing Dynea to store certain personal data of the employees for 60 years.

Appendix 1 contains specific guidelines in this regard. These guidelines are based on recommendations from HR Norge.

6.3 Special procedures for storing and deleting contact details for Business contacts

Personal data of Dynea's customers, suppliers and partners will not be stored longer than necessary to achieve the purpose of the processing of the personal data. However, customers that have not purchased products or services for a period, may be regarded as potential customers for the future, and serve as reference for previous communication, and these will still be available in our systems for further development of products, services and business relations.

Each Company and contact in Dyneas registers have an internal contact responsible (based on purpose) in our Global Address book (ERPsystem). This person is responsible for maintaining the contact persons of said company and conduct the deactivation process where the contact is no longer seen as relevant for conducting business. Personal data in Dynamics 365 are deactivated, not deleted, when they are no longer needed. This is due to the need to retain communication.

In addition, a systematic internal revision of Companies contact persons is due every two years.

Appendix 1 – Deletion Routines for HR information

DOCUMENT	STORAGE TIME
CV	For the duration of employment
Application	For the duration of employment
Certificates	For the duration of employment
Diplomas	For the duration of employment
Reference checks	For the duration of employment
Minutes from interviews/internal assessments	For the duration of employment
Personality and aptitude tests	For the duration of employment
Employment agreement including confidentiality agreement	10 years
Statement of consent to use of images etc.	For the duration of employment or until retracted
Leaves of absence	10 years
Salary history	10 years
Tax deductions	10 years
Garnishment of wages	5 years
Salary slip	5 years
Time sheets/overtime	For the duration of employment
Travel expense reports/disbursements	5 years
Sick leave	5 years
Follow-up of sick leave	For the duration of employment
Whistleblowing/whistleblower report	10 years
Cautions	5 years
Course diplomas	For the duration of employment
Development plans	For the duration of employment
Employee evaluations	For the duration of employment
Manager evaluations	For the duration of employment
Employee surveys	10 years
Profile pictures	For the duration of employment
Situational images	10 years
Mailbox with "Out of Office"-reply	3 months
Dismissal by AT or AG, with and without notice	10 years

Severance agreement	10 years
Employee reference letter	10 years
Exit interview	5 years
Register of exposed workers with related information	60 years