Appendix 6 Data Processing Agreement

Data Processing Agreement V.2E.1.3

Parties in this agreement are stated in the "Terms-of-Use Agreement".

Simployer Solutions AS is Data Processor when services described in appendix 1 (licensed services) are processing personal data.

Simployer AS is Data Processor when services described in appendix 2 (establishment and consultancy) are processing personal data.

1. Background

By entering into this Data Processing Agreement, the parties agree that the Data Processing Agreement shall enter into force. If the Data Processing Agreement has to be amended as a result of The EU General Data Protection Regulation (EU regulation no. 2016/679, hereafter "GDPR") and/or the Norwegian implementation of GDPR, the parties agree to cooperate on such an amendment by the Data Processor incorporating such necessary adjustments and immediately notifying the Data Controller.

The above-mentioned regulations contain requirements for the governing of the relationship between the Data Processor and the Data Controller, and the security and organizational measures that shall be implemented to ensure the legal and safe processing of personal data. This Data Processing Agreement is therefore entered into to ensure that personal data are processed in accordance with the regulations.

The Data Processing Agreement regulates the processing of personal data by the Processor on behalf of the Controller, as stated in this Data Processing Agreement.

The term "personal data" in this Data Processing Agreement shall have the same meaning as defined in the GDPR Article 4 (1): "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

This Data Processing Agreement is part of the following set of agreements and assumes that the following agreements are entered into or signed for the Data Processing Agreement to be valid:

- Agreement on the purchase of systems and/or manuals (hereinafter "Terms-of-Use Agreement"), including standard terms
- Service Level Agreement

2. Purpose

The purpose of the system and the Data Processor's processing of personal data is to enable the Data Controller to carry out actions related to HR issues.

The Data Controller has the right to use the system, and the Data Processor shall facilitate the Data Controller's processing of data by way of the system.

The system has functionality, depending on the module, for storing, e.g., the following types of personal data:

- Personnel records – Information about employees, access control, message archive, and organizational charts.
- Document archive – Documents relating to employees.
- Vacation – Information about holiday for employees.
- Days off and leave – Information about days off and leave for employees.
- Sick leave – Information about sick leave for employees and statutory documentation for follow-up.
- Deviation – Information about deviation from approved routines in the company. This may involve personal data about employees.
- Travels and expenses – Travels and expenses with documentation and attestations for employees.
- Processes (Onboarding, Offboarding, HSE) – Information about workflow and metadata related to defined processes in the company.
- Employment agreements – Information related to employment agreements in the company.
- Hour registration – Information related to hours worked for employees.
- Resource planning – roster for individuals.
- Learning – Management of education, including enrolment and course history, as well as management of knowledge tests, e-learning programs.
- Dialogue – Functionality for planning and conducting development dialogues or other structured dialogues.
- Competence management – Support for managing competence, individual competence mapping and profiling of individuals against required competence roles.
- Objectives – Managing goals and work objectives, with follow-up at individual level.
- Succession – Functionality to evaluate and plan work on successors, e.g. through the planning of replacements and rating of performance and risk.
- Chatbot – Digital assistant which answers user questions related to Simployer Handbooks.

The types of personal data processed under this Data Processing Agreement depend on which modules the Data Controller has ordered. The specific modules ordered are stated in the Terms-of-Use Agreement.

In connection with the establishment and use of the system, personal data may be registered in the system.

The Data Controller is responsible for the registration of personal data in the system after delivery, and any withdrawal and use of stored information.

The Data Processor is responsible for ensuring that the data is stored in a proper manner and later deleted or anonymized in accordance with this Data Processing Agreement.

The Data Processor is entitled to collect, extract, compile, analyse and otherwise process any information not defined as "Personal Data" under GDPR Art. 4 (1), and which is not otherwise protected by law or agreement between the parties. Such information that is not defined as "Personal Data" includes, but is not limited to anonymized data, volume data, frequency measurements, and other information that the Data Controller and its users and recipients generate in connection with the use of the system and the Data Processor's services, hereinafter referred to collectively as "Service Data". The Data Processor has the ownership of such Service Data and may be used by the Data Processors for legitimate business purposes without any obligations to the Data Controller or its users or recipients. The parties' duties and rights relating to the processing of personal data under this Data Processing Agreement and affiliated agreements do not apply to the processing of Service Data as described in this section.

For the record, “Service Data” does not include data that is the property of the Controller, i.e. data that is registered into the system by the users of the Controller, or data registered into the system by way of integrations with the Controller’s third party systems, referenced as “Customer data”.

3. Obligations of the Parties

3.1 Obligations of the Data Processor

The Data Processor is obliged to comply with requirements for Data Processors as provided by the Norwegian Personal Data Act, with regulations, including GDPR.

The Data Processor shall process personal data according to the agreed specified purposes pursuant to this Data Processing Agreement. The Data Processor shall not process personal data beyond the requirements for the purposes specified in this Data Processing Agreement without prior written agreement with the Data Controller or written instructions from the Data Controller.

The Data Processor shall, as far as is required under GDPR, assist the Data Controller in:

- Providing information to the Data Controller required in order to demonstrate that the obligations set out in GDPR art. 28 (3) are fulfilled.
- To a reasonable extent, helping the Data Controller to fulfil the Data Controller's obligation to respond to requests submitted by the Data Subject for the purpose of exercising his/her rights set out in Chapter III.
- To a reasonable extent, helping the Data Controller to fulfil the Data Controller's obligations according to GDPR art. 32-36, including non-conformance management.

The Data Processor shall notify the Data Controller if the Data Processor believes that an instruction from the Data Controller is in violation of the applicable privacy regulations.

All assistance should be carried out to the extent required by the Data Controller's need, the nature of the Processing and the information available to the Data Processor. All assistance and work in accordance with new and agreed instructions from the Data Controller may be invoiced to the Data Controller according to the rates stated in the Terms-of-Use Agreement and/or Service Level Agreement, unless otherwise expressly stated in this Data Processing Agreement or is limited by law.

The Data Processor is subject to confidentiality regarding documentation and personal data that he/she has access to in accordance with this Data Processing Agreement. This provision also applies after the termination of the Data Processing Agreement.

The Data Processors shall not disclose personal data to external parties unless otherwise follows from this Data Processing Agreement, have been agreed in writing, or such disclosure is required by law. Personal data processed by the Data Processor on behalf of the Data Controller may be transferred to countries in which the Data Processor, its sub-data processor or the sub-data processor's sub-data processor, conducts its activities in accordance with the provisions on use of subcontractors in section 4.

3.2 Obligations of the Data Controller

The Data Controller is obliged to comply with the requirements for Data Controllers as provided by the Norwegian Personal data Act, with regulations, including the GDPR.

The Data Controller confirms that:

I. There is sufficient legal basis for processing personal data;
II. The Data Controller is entitled to and responsible for the legality of the transfer of personal data to the Data Processor;
III. The Data Controller is responsible for the accuracy, integrity, content, reliability and legality of the personal data being processed;
IV. The Data Controller has informed the Data Subjects in accordance with the current legal requirements;
V. This Data Processing Agreement contains all instructions from the Data Controller at the time of signing the agreement.

The Data Controller shall ensure that personal data is processed in accordance with the GDPR, respond to inquiries from the Data Subjects and ensure that adequate technical and organizational measures are implemented to secure the Personal Data being processed, cf. GDPR Article 32.

The Data Controller is obliged to report data breach to the relevant supervisory authorities and, if applicable, to the Data Subject without undue delay in accordance with applicable legislation.

The Data Controller is responsible for ensuring that custom data fields in their own right, or by their content do not violate any applicable laws and regulations, including regarding personal data. The same applies to the use of combinations of data fields in, for example, reports, etc.

Where the system contains texts, data or other information, etc., which is owned/disposed by the Data Controller, the Data Controller warrants having full ownership or disposal rights for such texts, data, information, etc. and that neither storage nor the actual use of this material implies an infringement of third party rights or violates any law, regulation or other legal rules.

The Data Controller is subject to confidentiality regarding the documentation and personal data that he/she has access to in accordance with this Data Processing Agreement. This provision also applies after the termination of the Data Processing Agreement.

User ID and passwords for access to the system are created and administered by the administrator at the Data Controller. The Data Controller is obliged to ensure that passwords are stored and handled in such a way that only persons entitled to use under the Terms-of-Use Agreement, and that are authorized by the Data Controller, has access to the system. The Data Controller is responsible for the fact that his/her own employees only use the personal data in the system to perform assigned/permitted tasks.

The Data Controller handles and processes inquiries from the Data Subjects regarding access, rectification and deletion, etc.

4. Use of subcontractors

The Data Processor uses subcontractors to fulfil parts of its various obligations, including physical operation of the system. The Data Processor is responsible for the performance of the subcontractor's tasks in the same way as if the Data Processor himself was responsible for the execution.

The Data Processor is obliged to have separate data processing agreements with all its subcontractors to ensure fulfilment of the terms of this Data Processing Agreement and GDPR Art. 28.

Upon entering into this Data Processing Agreement, the Data Controller accepts the use of the following subcontractors:

Name of subcontractor	Description of processing	Location (storage and access)
Simployer AS	Development and operation of modules	Norway
Simployer Sweden AB	Development and operation of modules	EU
Simployer Tech Sp.z.o.o.	Development and operation of modules	EU
Rejlers Embriq AS	Operation of servers, firewall, antivirus and backup	Norway
Smart IT	Operation of servers, firewall, antivirus and backup	Norway
Elasticsearch Inc	Operation of Elastic search engine	EU
Microsoft Azure	Operation of servers, firewall and antivirus	EU
Sendgrid Inc.	Emailing	USA – transfers based on Binding Corporate Rules (BCR) and Standard Contractual Clauses (SCC)
Mailjet Inc	Emailing	EU
Signicat AS	Digital signature	EU
Auth0	Authentication	EU
Kindly AS	Operations of platform for machine learning and language technology	Norway – Kindly AS – processing and transfer of chat-data to subcontractors EU – hosting for temporary storage and processing of chat data

If the Data Processor changes or includes new subcontractors, the Data Controller shall be notified of this 90 calendar days before the new subcontractor starts processing personal data and the Data Controller may within 30 calendar days oppose the change. If the Data Controller opposes the change, the Data Controller may terminate the Terms-of-Use Agreement with 60 calendar days' notice. Notification of termination must be given at the same date as the Data Controller opposes the change. If the Data Controller does not terminate the Terms-of-Use Agreement, the new subcontractor is deemed to be accepted.

In case of change of a subcontractor, the former subcontractor must confirm in writing to the Data Processor that all personal data has been permanently deleted from its systems.

If the Data Processor is to enter into an agreement with Subcontractors in countries outside the EU/EEA, this should only be done according to valid mechanisms for such transfers such as EUs model clauses for the transfer of personal data to third countries or other applicable basis for transfer to third countries in accordance with GDPR Chapter 5. The same applies even if Personal Data is retained or stored in the EU/EEA when personnel with access to the data are located outside the EU/EEA.

5. Personal data security

The Data Processor shall ensure, through appropriate planned, systematic, organizational and technical measures, adequate information security in terms of confidentiality, integrity and availability in connection with the processing of personal data in accordance with GDPR Article 32.

The Data Processor should be able to document security measures. The documentation must be made available at the Data Controller's request.

The Data Processor shall ensure satisfactory personal data security regarding:

- confidentiality, i.e., the data is not available to persons who do not have legal access to the data,
- integrity, i.e. the data is not changed in an unauthorized or unintended manner and
- availability, i.e. the data is available and operative for legitimate and authorized use.

The Data Processor shall have routines and systematic processes to follow up on violations of personal data security ("Deviation"). If the Deviation is caused by the Data Controller, or circumstances within the control of the Data Controller, the Data Processor may invoice the Data Controller for work related to follow-up of the Deviation in accordance with the rates stated in the Terms-of-Use Agreement and/or the Service Level Agreement.

The Data Processor shall, without undue delay, notify the Data Controller of the Deviation.

The Data Processor shall provide the Data Controller with the necessary information to enable the Data Controller to comply with applicable laws regarding the processing of Personal Data and to enable the Data Controller to respond to requests from data supervisory authorities in the event of Deviations. It is the responsibility of the Data Controller to report nonconformities to the Norwegian Data Protection Authority in accordance with applicable legislation.

The Data Processor will not disclose passwords to the Data Controller's users without the Data Controller requesting this in writing. All passwords to Data Controller's users are stored with irreversible encryption, and it is physically impossible for the Data Processor to disclose passwords in plain text.

The Data Processor provides system backups and data according to current Service Level Agreement (SLA).

If personal data is to be transmitted electronically internally at the Data Controller or from the Data Controller to the Data Processor, the Data Processor recommends that transmission is done in encrypted form or otherwise secured by further agreement with the Data Processor.

6. Security audits

The Data Controller acknowledges that the Data Controller's right to conduct audits under GDPR is fulfilled through the fact that the Data Processor ensures that an independent third party, appointed by the Data Processor, performs a systemic audit of the system on a regular basis. The main results of the audit are made available to the Data Controller on request.

7. Liability and limitation of liability

Claims from a party as a result of the other party's failure to comply with the Data Processing Agreement shall be subject to the same liability regulations and limitations of liability as provided by the Terms-of-Use Agreement.

8. Duration of the Data Processing Agreement

This Data Processing Agreement shall apply from the date it has been signed by both parties until the Terms-of-Use Agreement expires or until the Data Processor's obligation to perform services under the Terms-of-Use Agreement terminates for any reason, except for the provisions of the Terms-of-Use Agreement and the Data Processing Agreement that continue to run after termination.

In the event of a material breach of the Data Processing Agreement, the Data Controller may impose on the Data Processor to stop further processing of personal data with immediate effect. The Data processor can, for the same reasons, stop all processing on behalf of the Data Controller with immediate effect. Deletion of data covered by this Data Processing Agreement will however not be implemented until the Terms-of-Use Agreement expires in accordance with paragraph 9 below.

9. Upon termination

After the expiry of the Terms-of-Use Agreement, the Data Processor is obligated to anonymize all personal data covered by this Data Processing Agreement, and subsequently delete all the customers data. Anonymization means that the data is no longer personal data and therefore not covered by the privacy policy. The Data Processor shall provide the Data Controller with a written statement, after which the Data Processor guarantees that all personal data or data mentioned above has been anonymized and that the Data Processor has not retained any copy, print or retained personal data in any other medium.

The Controller is upon termination of the Terms-of-Use Agreement entitled to receive Customer data in return. The way return of Customer data should be handled is governed by the Service Level Agreement (SLA).

10. Notices

Notices pursuant to this Data Processing Agreement shall be sent in writing to the Data Controller's contact person as specified in the Terms-of-Use Agreement.

11. Amendment of the Data Processing Agreement

The Data Processor may amend the content of the Data Processing Agreement if the Data Controller is notified about this 90 calendar days before the amendment enters into force. The Data Controller can oppose the amendment within 30 calendar days. If the Data Controller opposes the amendment, the Data Controller may terminate the Terms-of-Use Agreement with 60 calendar days' notice. Notice of termination must be given at the same date as the Data Controller opposes the amendment. If the Data Controller does not notify termination of the Terms-of-Use Agreement, the amendment is deemed to be accepted.