Data Processing Agreement (DPA)

Version 3.0 | Appendix 3 to Master Subscription Agreement

APPENDIX 3 - Data Processing Agreement

Version 3.0

1. Background

1.1. This Data Processing Agreement (DPA) governs Simployer's processing of personal data as a processor on behalf of the Customer as the controller.

1.2. Where a term used in this DPA is defined in Article 4 of the GDPR, such term shall have the meaning ascribed to it in Article 4 of the GDPR.

2. Purpose

2.1. The purpose of the processing of personal data under this Agreement is to provide the Customer with the Subscription Services and enable the Customer to carry out actions related to HR management and administration.

2.2. The categories of data subjects and types of personal data processed through the Subscription Services may vary depending on the specific modules procured by the Customer, as set out in the Order Form. The relevant information is set out on Simployer's Trust Center (Subprocessors used by Simployer).

3. Obligations of the parties

3.1 Obligations of Simployer

3.1.1 Simployer shall process personal data according to the agreed specified purposes pursuant to this DPA. Simployer shall not process personal data beyond the requirements for the purposes specified in this DPA without prior written agreement with or written instructions from the Customer.

3.1.2 Simployer shall, as far as is required under GDPR, assist the Customer with:

- Providing information to the Customer required in order to demonstrate that the obligations set out in GDPR art. 28 (3) are fulfilled.
- To a reasonable extent, helping the Customer to fulfil the Customer'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 Customer to fulfil the Customer's obligations according to GDPR art. 32-36, including non-conformance management.
- Simployer shall notify the Customer if Simployer believes that an instruction from the Customer is in violation of the applicable privacy regulations.

3.1.3 All assistance should be carried out as Professional Services and to the extent reasonably required by the Customer's need, the nature of the Processing and the information available to Simployer. All assistance and work in accordance with new and agreed instructions from the Customer may be invoiced to the Customer according to

Simployer's at any time applicable list prices, or the rates agreed in the Order Form, unless otherwise expressly stated in this DPA or is limited by Law.

3.1.4 Simployer is subject to confidentiality regarding documentation and personal data that it has access to in accordance with this DPA. This provision also applies after the termination of the DPA.

3.1.5 Simployer shall not disclose personal data to external parties unless otherwise follows from this DPA, have been agreed in writing, or such disclosure is required by Law. Personal data processed by Simployer on behalf of the Customer may be transferred to countries in which Simployer, its sub-processors or the sub-processor's sub-processor, conducts its activities in accordance with the provisions on use of sub-processors in section 4.

3.1.6 Simployer is responsible for ensuring that the data is stored in a proper manner and later deleted or anonymized in accordance with this DPA.

3.2 Obligations of the Customer

3.2.1 The Customer is obliged to comply with the requirements for data controllers as provided by the relevant national legislation implementing the GDPR including underlying regulations, and the GDPR.

3.2.2 The Customer confirms that:

- There is sufficient legal basis for processing personal data;
- The Customer is responsible for the legality of the transfer of personal data to Simployer;
- The Customer is responsible for the accuracy, integrity, content, reliability and legality of the personal data being processed;
- The Customer has informed the data subjects in accordance with the current legal requirements;
- This Data Processing Agreement contains all instructions from the Customer at the time of signing the agreement.

3.2.3 The Customer 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, in accordance with GDPR Article 32.

3.2.4 The Customer 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.

3.2.5 The Customer 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.

3.2.6 If the Customer intends to use the service also for employees of companies other than their own, they shall on their own obtain the companies' permission to process personal data about the affected employees. In the case of companies and employees residing outside the EU/EEA, the Customer shall independently supervise and be responsible for compliance with legal requirements in accordance with applicable foreign Law.

4. Use of sub-processors

4.1. Simployer uses sub-processors to fulfil parts of its various obligations, including hosting of the systems. Simployer is responsible for the performance of the sub-processor's tasks in the same way as if Simployer itself was responsible for the execution.

4.2. Simployer is obliged to have separate data processing agreements with all its subcontractors to ensure fulfilment of the terms of this DPA and GDPR Art. 28.

4.3. The sub-processors relevant to the module procured by the Customer, as specified in the Order Form, are listed at Simployer's Trust Center. The link will be kept up-to-date to reflect any changes in sub-processor engagement.

4.4. The Customer shall be notified of any changes or addition of new sub-processors at least thirty (30) calendar days before the change is effective or the new sub-processor are given access to personal data. The Customer must object in writing to the change within 30 calendar days. Unless the Customer objects in writing within the deadline, the Processor may use the new sub-processor for the indicated data processing activities. If the Customer reasonably objects within the given timeline, Simployer will use reasonable efforts to change the Subscription Services to avoid processing of the personal data by the "objected-to" new sub-processor. If Simployer is unable to implement such changes within a reasonable period of time, which shall not exceed thirty (30) days from receipt of the Customer's written objection, the Customer shall have the right to terminate the relevant parts of the Subscription Services. Simployer shall refund the Customer for any prepaid amounts corresponding to the unused portion of the Subscription Services from the effective date of termination. The Customer's termination notice must be sent within fourteen (14) calendar days from Simployer's confirmation that Simployer's notice that it cannot avoid using the objected-to sub-processor, otherwise the Customer shall be deemed to have consented to the proposed sub-processing.

4.5. Any transfer of personal data to sub-processors in countries outside the EU/EEA and which are not recognized by the European Commission as providing an adequate level of protection for personal data shall only be done according to valid mechanisms for such transfers such as EU's 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.

5. Information security

5.1. Simployer 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.

5.2. Simployer should be able to document security measures. The documentation must be made available at the Customer's request.

5.3. Simployer 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.

5.4. Simployer shall have routines and systematic processes to follow up on violations of personal data security ("Deviation"). If the Deviation is caused by the Customer, or circumstances within the control of the Customer, Simployer may invoice the Customer for work related to follow-up of the Deviation as Professional Services in accordance with Simployer's at any time applicable list prices, or the rates agreed in the Order Form.

5.5. Simployer shall, without undue delay, notify the Customer of the Deviation.

5.6. Simployer shall provide the Customer with the necessary information to enable the Customer to comply with applicable laws regarding the processing of Personal Data and to enable the Customer to respond to requests from data supervisory authorities in the event of Deviations. It is the responsibility of the Customer to report nonconformities to the relevant supervisory authority in accordance with applicable Law.

6. Security audits

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

7. Duration of the DPA

7.1. This DPA shall apply from the date when the relevant Order Form is signed by both parties and until the Agreement expires or until Simployer's obligation to perform the Subscription Services terminates for any reason, except for the provisions of the Agreement that continue to run after termination.

8. Upon termination

8.1. After the expiry of the Agreement Simployer is obligated to anonymize all personal data covered by this DPA, and subsequently delete all the personal data for which the Customer is the controller. Upon request, Simployer shall provide the Customer with a written statement, after which Simployer guarantees that all personal data or data mentioned above has been anonymized and that Simployer has not retained any copy, print or retained personal data in any other medium.

8.2. The Customer may access its personal data upon termination of the Agreement in accordance with the T&Cs.

9. Notices

9.1. Notices pursuant to this DPA shall be sent in writing to the Customer's contact person as specified in the Order Form.

Appendix A – Insights / Integration Interface ("API")

Appendix A only applies if the Customer has purchased access to Insights (an integration Interface), hereinafter referred to as the "API". Simployer APIs expose integration interfaces that selected Users at the Customer's side can access, which enables the Customer to transfer information, including personal data, from the Customer's data generated in Simployer, for further processing and analysis in third-party software.

The API is protected by an API key that is used to authenticate the individual service(s) that will interact with the interface. The Customer is provided with this key and is solely responsible for using it and to only authenticate the systems, and those users, who shall have access to the service.

The interface allows for access to the Customer's data, including personal data registered or generated in the system and the Customer's database, and does not have the same access control and mechanisms to ensure privacy that is built into Simployer by default. It is therefore very important that the Customer only uses the service for purposes, and only authenticates systems and users against the interface, which the Customer has made necessary assessments of (legal and technical assessments).

Simployer is responsible for the availability and confidentiality of data up and until the endpoints. After data has left the endpoint, it is the Customer who is responsible for all use of the service and all use of data made available via the endpoint. Simployer, including subcontractors, do not have any responsibility for customer's use of the endpoints or Customer's processing of data obtained from the endpoints, or the integrity of data submitted to the endpoints (from the Customer's systems or other third parties the Customer is responsible for).

Where integrations do not use endpoints for transferring data but instead use file-based transfer of data, the same principles apply as mentioned above.

Appendix B – Engagement Module

Appendix B only applies if the Customer has purchased the engagement module. Regarding the disclosure of data from this module, Simployer cannot provide the Customer with response information in any other way than in anonymized and de-identified form. Response information means the answers employees have given to employee surveys collected using the Engagement module.

The Customer is also responsible for ensuring that their use of-, and the content of the questions and answers stored in the Engagement module. The Customer should avoid and or exercise caution in asking questions that involves, or results in, response information that contains personal data and that they do not need, or have legal grounds to process.

Appendix C – Whistleblowing Module

Appendix C only applies if the Customer has purchased the whistleblowing-module and activated it for use.

In support of the EU Directive 2019/1937 on Whistleblowing, Simployer offers a digital service to facilitate and support the process of whistleblowing.

The service enables all individuals who know the address of the whistleblowing functionality at the customer, to submit whistleblowing. This could include persons also outside of their own company. The whistleblower can choose to submit the message with their name and contact details, or to remain anonymous.

The Customer is responsible for ensuring that the messages are processed and stored in accordance with applicable regulations, i.e. both the national whistleblower-regulation and the rules of the GDPR. The system automatically deletes data in messages two years after it was created, but deletion should otherwise be done by the administrator of the module, and should be done continuously and without undue delay.