

Appendix 1: Terms and conditions regarding the processing of personal data

1 Definitions

"Data Protection Legislation" means the current Personal Data Act (523/1999) until 25 May 2018 and the GDPR and any national laws and regulations giving effect to the GDPR and any other legislation which applies to the Processing of Personal Data, in each case to the extent it applies to this Agreement;

"GDPR" means the General Data Protection Regulation of the European Union (2016/679/EU);

"Personal Data" means any information relating to an identified or identifiable natural person. 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;

"Personal Data Breach" means an event leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data Processed;

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2 General

This Data Processing Appendix ("**DPA**") sets out the terms and conditions under which the Supplier processes the Customer's Personal Data. The purpose of this DPA is to take into account the responsibilities and obligations set by the GDPR.

The Customer is the data controller of the Customer's Personal Data Processed in connection with the service agreed in the Agreement. As a data controller, the Customer determines the purposes and means of the Processing of Personal Data. The Supplier is the data processor, who Processes the said Personal Data on behalf of and by the order of the Customer as agreed in this DPA. The Parties shall agree more specifically in [Schedule 1.1](#) on the categories of data subjects, categories of Processing carried out by Supplier, data security procedures and the purpose for which the Supplier Processes the Customer's Personal Data.

The Parties understand that authorities may issue orders and guidelines within the scope of the GDPR after the signing of the Agreement. The Parties commit to, if necessary, amend this DPA based on such orders and guidelines.

The Parties shall inform each other of the contact details of their possible data protection officers.

3 Responsibilities of the Customer

The Customer shall process the Personal Data in compliance with the Data Protection Legislation and the Customers' written instructions. The Customer is responsible for the lawfulness and completeness of the instructions on the Processing of Personal Data set out in [Schedule 1.2](#) and that there are no defects or errors in the said instructions. Possible changes to the instructions set out in [Schedule 1.2](#) and the cost effects of such changes shall always be agreed on separately in writing.

The Customer is responsible for the Personal Data provided to the Supplier and the lawfulness of the Processing during the whole term of this DPA. The Customer is responsible for providing all appropriate notices and information related to the Processing of Personal Data to the data subjects in accordance with applicable laws. The Supplier does not monitor the content, quality or timeliness of the Personal Data provided by the Customer.

The Customer shall ensure that the purpose and grounds for Processing are in compliance with the Data Protection Legislation. The Customer shall also ensure that Personal Data has been collected in accordance

with the Data Protection Legislation and that the Customer has the right to transfer the Personal Data to be Processed by the Supplier.

The Parties do not intend to transfer any of the controller's legal obligations to the processor with this DPA.

4 Responsibilities of the Supplier

The Supplier shall Process the Personal Data in accordance with the Data Protection Legislation and the written instructions set out in Schedule 1.2, unless otherwise required by law applicable to the Supplier. In such case, the Supplier shall inform the Customer of such legal requirement before the Processing, unless the applicable law prohibits such notification. For the sake of clarity, the Customer will always be deemed to have instructed the Supplier to provide the services related to the Processing of Personal Data agreed under the Agreement.

Taking into account the nature of the Processing, the Supplier shall assist and support the Customer with appropriate technical and organisational measures chosen by the Supplier so that the Customer can fulfil its obligation to respond to requests concerning the exercise of the following rights of the data subjects, as set out in Chapter III of the GDPR (provided that the data subject has the said right under the GDPR):

- a) right of access to the Personal Data;
- b) right to rectification and erasure;
- c) right to restriction of Processing;
- d) right to Personal Data portability; and
- e) right to object to Processing of Personal Data.

In case a Party receives a request concerning the use of the data subject's rights, the Party receiving the request shall notify the other Party of the request immediately and at the latest on the first weekday following the receipt of the request, if fulfilment of the request requires any actions from the other Party. The notification will contain all information necessary to the other Party to fulfil the request. The Supplier is entitled to charge the Customer for all actions taken to fulfil the request of the data subject on a time and material basis in accordance with its price list applicable at the time.

Taking into account the nature of the Processing and the information available to the Supplier, the Supplier shall assist the Customer in ensuring compliance with the following obligations under Articles 32-36 of the GDPR:

- a) ensuring the security of Processing by implementing appropriate technical and organisational measures;
- b) notification of Personal Data Breaches to supervisory authority and the data subjects;
- c) participating in data protection impact assessment if such impact assessment is necessary under Article 35 of the GDPR; and
- d) participating in the prior consultation of the supervisory authority if such prior consultation is necessary under Article 36 of the GDPR.

The Supplier shall assist the Customer only to the extent required of a data processor in the Data Protection Legislation. The Supplier is entitled to charge the Customer for the aforementioned measures on a time and material basis in accordance with its price list applicable at the time.

5 Data Security

The Parties undertake to implement the technical and organisational measures commonly used in the industry to protect the Personal Data. In connection with agreeing on the implementation of such measures, the Parties shall in planning and implementation take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. When assessing appropriate level of security, the Parties shall also take into account the risks of the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

Such measures include e.g.:

- a) pseudonymisation and encryption of Personal Data;
- b) the ability to ensure the continuing confidentiality, integrity, availability and resilience of processing systems and services;
- c) the ability to restore the availability of and access to Personal Data in a timely manner in the event of a physical or technical incident; and
- d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures to ensure the security of data Processing.

The aforementioned measures are examples of how the Parties may ensure the security of the Processing of Personal Data. The Parties shall separately agree in Schedule 1.1 on the aforementioned measures or other data security procedures that the Supplier shall implement in the Processing of Personal Data. The Customer shall ensure appropriate and sufficient data security of the equipment and IT environment under its control. Unless agreed otherwise in the Agreement, the Customer shall be responsible for taking backups of the Personal Data and the verification of the functionality of the backups.

The Customer shall inform the Supplier of all issues related to the Personal Data provided by the Customer, such as risk assessment and the inclusion of special categories of Personal Data, which issues affect the technical and organizational measures implemented under this DPA. For the sake of clarity, possible changes to the data security procedures agreed in Schedule 1.1 and the cost impacts of such changes will always be agreed separately in writing.

The Supplier shall ensure that the persons Processing Personal Data are committed to confidentiality or are under an appropriate statutory obligation of confidentiality. The Supplier shall implement necessary measures to ensure that the said persons only process Personal Data in accordance with the instructions set out in Schedule 1.2.

6 Transfer of personal data

Unless otherwise agreed in Schedule 1.2, the Supplier has the right to transfer Personal Data outside the EU or EEA in accordance with the Data Protection Legislation. The Supplier shall be entitled to transfer the Personal Data freely within the EU or EEA for the purpose of providing the agreed service.

7 Subcontractors

The Customer gives general authorisation to the Supplier to use subcontractors in the provision of the service and the related Processing of Personal Data. The subcontractors used in the Processing of Personal Data at the time of signature of the Agreement are listed in Schedule 1.1. The Supplier shall be responsible that its subcontractors Process the Personal Data in accordance with this DPA and the Data Protection Legislation.

The Supplier shall notify the Customer if it plans on changing or adding subcontractors participating in the Processing of Personal Data. The Customer is entitled to object to such changes on reasonable grounds. The Customer shall notify the Supplier of the objection without undue delay after receiving the said notice from the Supplier. Should the Customer not accept the change or the addition of a subcontractor, the Supplier has the right to terminate the Agreement with 30 days' notice.

In addition to the subcontractors listed in Schedule 1.1, the Supplier is entitled to use business partners for the purposes of customer service, maintenance of customer relationships, communications, marketing and development. The Customer is entitled to request an up-to-date list of such subcontractors. The business partners of the Supplier may Process the Customer's Personal Data only for measures carried out on behalf of the Supplier for the purposes determined in the Agreement. The Supplier shall always ensure that its partners do not Process the Personal Data transferred to them for any other purposes.

8 Personal Data Breaches

Each Party shall notify the other Party without undue delay, if it becomes aware of a Personal Data Breach. When notifying the Supplier of a Personal Data Breach, the Customer shall provide to the Supplier all information that can be deemed to help in the investigation, restriction and prevention of the Personal Data Breach. The Parties may separately agree on the notification procedure more specifically. Unless otherwise agreed by the Parties, the notification will be made to the contact person informed by each Party.

When notifying the Customer of a Personal Data Breach the Supplier shall, to the extent such information is available to the Supplier, provide the Customer with the following information:

- a) a description of the nature of the Personal Data Breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned (as far as the information is available to the Supplier);
- b) the contact information of the Supplier's data protection officer or other contact point where more information can be obtained;
- c) a description of the likely consequences of the Personal Data Breach; and
- d) a description of the measures taken by the Supplier to address the Personal Data Breach and the measures taken by the Supplier to mitigate the adverse effects of the Personal Data Breach.

If the Personal Data Breach is caused by a reason that is under the responsibility of the Customer, the Customer shall be liable for the Supplier's costs resulting from the Personal Data Breach. The Customer shall be responsible for notifying the supervisory authority and the data subjects of the Personal Data Breach as set out in the GDPR.

9 Records of processing activities

The Supplier shall maintain a record of Processing activities carried out behalf of the Customer. The record contains the following information:

- a) the name and contact details of the Customer, the Supplier and the Supplier's possible data protection officer and information about possible subcontractors;
- b) the categories of Processing carried out behalf of the Customer;
- c) information on transfers of Personal Data outside the EU or EEA; and
- d) where possible, a general description of the technical and organisational safety measures implemented in accordance with section 5 of this DPA.

10 Right to audit

During the term of the Agreement, the Customer or an independent third party auditor appointed by the Customer, which third party may not be the Supplier's competitor, will have the right to audit the Supplier's compliance with the obligations addressed to it under this DPA. The subject of the audit will be the Supplier's

relevant material related to the Processing of the Customer's Personal Data and the Supplier's systems and premises used in the Processing of Customer's Personal Data. The audit may be carried out no more than once per year, during the Supplier's normal business hours and the Supplier shall be notified of the audit in writing at least 30 days in advance. However, the Supplier shall always allow the regulatory authority supervising the Customer's business to conduct audits targeted at the Customer's data processor's operations. The relevant parts of this DPA will be applied to such audits.

The Supplier shall participate in the audit and provide to the auditor information required to demonstrate the Supplier's compliance with the requirements addresses to it under this DPA. The audit may not interfere with the Supplier's operation of services and the auditor will not be entitled to access information of the Supplier's customers or partners. Should the Customer not be the one performing the audit, the auditor will enter into a confidentiality agreement with the Supplier prior to the execution of the audit.

The Customer shall bear all costs resulting from the audit and compensate the Supplier for all costs incurred as a result of the audit. If the audit reveals material deficiencies in the Supplier's performance, the Supplier shall bear its own cost resulting from the audit.

11 Termination of the processing of Personal Data

Upon termination of the Agreement and provision of service related to the Processing of Personal Data, the Supplier undertakes, in accordance with the Customer's written request, to delete the Personal Data from active databases or return the Personal data to the Customer. Additionally, upon termination of the Agreement, existing copies of the Personal Data shall be deleted in accordance with the backup and maintenance practices of the Supplier and its subcontractors, unless the Supplier is required to store the said Personal Data under applicable law or regulation. The Supplier is entitled to charge the Customer for the return or destruction of the Personal Data on a time and material basis in accordance with its price list applicable at the time. The Parties may agree more specifically on the practices related to the deletion or return of Personal Data.

12 Damage caused by the processing of Personal Data

If a data subject suffers damages due to a breach of the GDPR, each Party shall itself be liable for the damage caused to the data subject in accordance with Article 82 of the GDPR. Each Party shall also itself be liable for any administrative fines imposed by a supervisory authority to it in accordance with Article 83 of the GDPR.

The limitation of liability clause of the Agreement applies to any liability arising under this DPA.

13 Schedules

Schedule 1.1 Description of the Personal Data and data security procedures

Schedule 1.2 Instructions on the Processing of Personal Data

Schedule 1.1

Schedule 1.1: Description of the Personal Data and data security procedures

The Parties may amend or update this schedule in writing, if necessary.

1 The purpose of the processing

The Supplier shall process Personal Data only for the following purpose: Provision and maintenance of a process and digital documentation management and control system provided as a SaaS service, completion of orders related to the service, provision of support services and maintenance of customer relationships.

2 Contents of the processing

The Supplier shall perform the following Processing activities on the Personal Data:

- | | |
|--|--|
| <input checked="" type="checkbox"/> Collection | <input checked="" type="checkbox"/> Consultation |
| <input checked="" type="checkbox"/> Recording | <input checked="" type="checkbox"/> Use |
| <input checked="" type="checkbox"/> Organisation | <input checked="" type="checkbox"/> Making data available (disclosure of data by e.g. transmission or dissemination) |
| <input checked="" type="checkbox"/> Structuring | <input checked="" type="checkbox"/> Alignment or combination |
| <input checked="" type="checkbox"/> Storage | <input checked="" type="checkbox"/> Restriction |
| <input checked="" type="checkbox"/> Adaptation, alteration | <input checked="" type="checkbox"/> Erasure and destruction |
| <input checked="" type="checkbox"/> Retrieval | <input type="checkbox"/> Other processing operations: |

3 Categories of data subjects and Personal Data

The Supplier shall Process the following categories of data subjects and Personal Data:

Registered users

- a) Contact information, such as name, email address, phone number
- b) Information related to employment, such as employer, title, address of employer
- c) Identification information related to the provision and maintenance of the service, such as identifiable user ID, cookies required by the service, browser identification information (version etc.), mobile device identification information (brand, model etc.), IP address

Non-registered users

- a) Email address
- b) Identification information related to the provision and maintenance of the service, such as identifiable user ID, cookies required by the service, browser identification information (version etc.), mobile device identification information (brand, model etc.), IP address

Project contact persons

- a) Contact information, such as name, email address, phone number
- b) Information related to employment, such as employer, title, address of employer

4 Applicable data security procedures

The Supplier shall comply with its own data security guidelines when Processing Personal Data.

Schedule 1.1

5 Subcontractors of the Supplier

The Supplier uses the subcontractors specified in [LINK TO WEBSITE] in the Processing of Personal Data under this DPA.

Schedule 1.2

Schedule 1.2: Instructions on the Processing of Personal Data

The Customer has not provided the Supplier with any separate instructions on the Processing of Personal Data at the time of signature of the DPA.