**Schedule 1**
**Data Protection**

## 1. Definitions

In this Schedule 1 ("**Contract Data Processing Agreement**"), the following terms have the following meanings:

**"Data Protection Laws"** means the data protection laws of the country in which the Controller is located (including Regulation (EU) 2016/679 (General Data Protection Regulation - "**GDPR**")) and any other data protection laws applicable to the Controller in connection with the main agreement.

**"Personal Data"** means, as defined in the GDPR, information concerning an identified or identifiable natural person that is processed by the Processor in the course of providing services to the Controller pursuant to this Contract Data Processing Agreement.

**"Standard Clauses"** means the standard contractual clauses for the transfer of Personal Data from a Controller in the European Economic Area to Processors in third countries as set out in the Annex to European Commission Decision 2010/87/EU and supplemented by including the description of the Personal Data and the technical and organisational measures.

**"Subcontractors"** within the meaning of this provision are third parties instructed by the Processor to provide such services which directly relate to providing the main service. This does not include ancillary services which the Processor uses, for example, as telecommunications services, postal/transport services, maintenance and user service or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems.

"**Controller**", "**Data Subject**", "**Personal Data Breach**", "**Processor**" and "**Processing**" have the meanings set forth in the GDPR.

## 2. Processor's obligation to follow instructions

2.1 The Processor must process the Personal Data in accordance with the instructions from the Controller. A prior written agreement between the Parties is required for any further instructions that would result in Processing outside the scope of this Contract Data Processing Agreement (e.g. if a new purpose for processing is introduced).

2.2 The Processor will only disclose Personal Data to third parties (including authorities, courts or law enforcement agencies) if it has obtained written

permission from the Controller or is required to do so by law. If the Processor is required to disclose Personal Data to a law enforcement agency or other third party, it will notify the Controller prior to such disclosure (unless this is prohibited by law).

## 3. Processor's Personnel

The Processor will ensure that its employees authorised to process Personal Data have agreed to observe confidentiality by signing a contract. An obligation to observe confidentiality is only necessary if there are not already appropriate legal obligations of confidentiality.

## 4. Technical and organisational measures

4.1 The Processor must implement and maintain appropriate technical and organisational security measures ("**TOMs**") in accordance with the Schedule to prevent Personal Data Breaches and to be able to provide the support described in section 5.

4.2 The TOMs are subject to technical progress and further development. The Processor reserves the right to change the security measures taken.

## 5. Exercising rights of Data Subjects

5.1 If the Controller receives requests or notifications from Data Subjects in relation to the Processing of Personal Data ("**Request**"), the Processor will support the Controller in a reasonable manner and provide information upon Request.

5.2 The Processor must correct, delete or block Personal Data if instructed to do so by the Controller.

## 6. Supporting the Controller

6.1 The Processor will support the Controller in ensuring an adequate level of protection through technical and organisational measures.

6.2 In the event of a Personal Data Breach, the Processor must:

a) inform the Controller without undue delay after the breach has been established;

b) provide the Controller with necessary information, cooperation and assistance regarding the measures to be taken in response to a Personal Data Breach.

6.3 Where a data protection impact assessment ("**DPIA**") is required for the Processing of Personal Data under Data Protection Laws, the Processor will,

upon request, provide the Controller with the information and assistance reasonably required for the DPIA.

## 7. Deletion and return of Personal Data

7.1 Once the processing services have been completed, the Processor must, as the Controller chooses, either delete or return all Personal Data and delete any copies, unless it is required to continue to store them under applicable law.

7.2 If additional expenses are incurred due to deviating specifications when returning or deleting the Personal Data, they will be borne by the Controller.

## 8. Information rights and audit

8.1 Upon request, the Processor will provide the Controller with all information or certificates reasonably necessary to demonstrate compliance with the obligations set forth in this Contract Data Processing Agreement.

8.2 If the Processor does not provide sufficient information or certificates, or if required by Data Protection Law or by a competent authority, the Processor must enable and cooperate in the on-site audit of the Processor's Processing of Personal Data during normal business hours with reasonable notice. Such audit may not interfere with the Processor's business operations.

8.3 The Processor will forward to the Controller all requests from national data protection authorities relating to the Processing of Personal Data carried out by the Processor. The Processor will cooperate with the Controller in its dealings with national data protection authorities and audit requests received from them.

## 9. Obligation to report unlawful instructions from the Controller

The Processor must inform the Controller if it believes that an instruction breaches applicable data protection provisions. The Processor may suspend the implementation of the instruction until it has been confirmed or amended by the Controller. The Processor may refuse to implement instructions that are obviously unlawful. The Processor is not obliged to verify the lawfulness of the Controller's instructions.

## 10. Subcontracting relationships

10.1 The Controller agrees that the Processor may use subcontractors to carry out certain processing activities with regard to Personal Data.

10.2 The current subcontractors are listed in the Schedule.

10.3 If the Processor engages additional subcontractors or replaces or removes subcontractors, it will (i) inform the Controller of this in good time in advance and (ii) enter into a written contract with the subcontractor which imposes the obligations set out in Article 28 (3) and (4) GDPR on the subcontractor. The Controller may object to the engagement of subcontractors within 30 days in writing with appropriate justification if the engagement of a subcontractor violates this Contract Data Processing Agreement or Data Protection Laws.

10.4 The Processor's contract with the subcontractor must comply with the requirements of the Data Protection Laws, in particular Article 28 GDPR.

10.5 If the subcontractor fails to comply with its data protection obligations under the contract or Data Protection Laws, the Processor is liable to the Controller for performance of the Controller's obligations under the provisions of this Contract Data Processing Agreement.

## 11. International data transmission

11.1 The Processor will not transfer Personal Data to countries outside the European Economic Area ("**Third Country**") for Processing pursuant to this Contract Data Processing Agreement.

## 12. Contractual term and termination

12.1 This Contract Data Processing Agreement ends automatically when the main agreement ends. The Controller may exercise its rights under this Contract Data Processing Agreement as long as the Processor processes Personal Data.

12.2 Either Party may terminate the Contract Data Processing Agreement at any time with reasonable notice for good cause if the other Party commits a material breach of duty under this Contract Data Processing Agreement.

12.3 If the Controller objects to the removal or replacement of a subcontractor or to the involvement of a further subcontractors the Processor can stop providing the service to the Controller within four weeks of receipt of the objection and terminate the service agreement without notice and with immediate effect if the Processor cannot be reasonably expected to provide the service without the intended change.

## 13. Liability

13.1 If claims for damages are asserted against a Party due to the Processing of Personal Data, the Party against whom the claim is filed must inform the other Party without undue delay. This only applies to the Controller if the asserted claim is based on a breach of duty by the Processor.

13.2 The Controller will indemnify the Processor from all claims which third parties assert on the grounds of the breach of their rights against the Processor on the basis of the Processing of Personal Data instructed by the Controller unless the third-party claim is based on the Processing of Personal Data by the Processor contrary to instruction. However, nothing in this Contract Data Processing Agreement limits the liability of a Party for loss based on wilful misconduct or gross negligence of the Party. In all other respects, the liability provisions in the main agreement apply.

## 14. Miscellaneous

14.1 In the event of a discrepancy the provisions of this Contract Data Processing Agreement take precedence over the provisions of the main agreement between the Controller and the Processor.

14.2 None of the Parties will receive remuneration for performing its duties under this Contract Data Processing Agreement unless this is expressly stipulated in this Agreement or another agreement.

14.3 The Processor may charge reasonable remuneration for support when carrying out an audit at the Processor's premises in accordance with this Schedule. The time and effort required for an audit is generally limited to one day per calendar year for the Processor.

14.4 If "written" consent or other cooperation is required in accordance with this Contract Data Processing Agreement it may also be in text form (e.g. by email).

**Annex to Schedule 1**

*The definitions set out in the Agreement apply to this Schedule.*

1. Subject of the data processing

   The Personal Data are the subject of the following data processing: [**OPTION 1**: [FREE TEXT)

   [**OPTION 2**: The data processing and its purposes are described in the main agreement]

2. Categories of Data Subjects

   The following categories of Data Subjects are affected by the data processing:

   If applicable, predefined selection fields:

   ☐ Existing customers

   ☐ Interested parties/potential customers

   ☐ Newsletter subscribers

   ☐ Website users/visitors

   ☐ Applicants

   ☐ Interns/working students

   ☐ Employees (permanent staff, trainees, temporary workers, freelancers)

   ☐ Suppliers/subcontractors/contact persons

   [FREE TEXT

3. Categories of Personal Data

   The following categories of Personal Data are affected by the data processing:

   ☐ Master personnel data (esp. name, address, date of birth, telephone number)

   ☐ Contract master data (for example, contractual relationship, name, address of the contractual partner's staff, etc.)

   ☐ Address data (e.g. street, post office box, postcode)

   ☐ Communication data (e.g. email address, telephone number, mobile phone number)

   ☐ Photographs of Data Subjects

   ☐ Internet protocol address (IP address)

☐ Bank details (e.g. IBAN, BIC)

☐ Employee's salary

☐ Credit reports, creditworthiness and fraud alerts

☐ Information on employment relationship (history)

☐ Order data (from online shop)

☐ Email messages

[FREE TEXT

The following special types of Personal Data are affected by the data processing:

☐ Information on physical and mental health

☐ Information on medical care (e.g. test results, medication)

☐ Biometric identifiers (DNA, finger, iris and voice)

☐ Criminal charges, convictions and court files

☐ Information on sex life or sexual orientation

☐ Ethnic origin

☐ Religious or ideological beliefs

☐ Trade union membership

4. Subcontractor

The Processor intends to use the following subcontractors for the Processing of Personal Data. The Controller consents to the engagement of the following subcontractors in accordance with section:

| **Name of the subcontractor** | **Address** | **Work to be carried out** | **International transmission (if applicable)** |
|---|---|---|---|
| [FREE TEXT | [FREE TEXT | [FREE TEXT | [FREE TEXT |
| [FREE TEXT | [FREE TEXT | [FREE TEXT | [FREE TEXT |

5. Description of the technical and organisational measures

In order to ensure adequate protection of Personal Data through technical and organisational measures, the provider implements the following measures in particular, but not exclusively:

5.1 Information security programme

The Processor must maintain an information security programme that regulates the use of people, processes and technologies in the handling of Personal Data. This includes:

☐ The Processor must appoint one or more security officer(s) responsible for monitoring security policies and procedures.

☐ The Processor offers security training to ensure that employees are aware of security policies and procedures and their respective roles. The Processor will also inform staff of the possible consequences of non-compliance with security policies and procedures.

5.2 Access control

The Processor will ensure that unauthorised persons do not gain access to data processing equipment (in particular telephone systems, databases, application servers and connected hardware) used for the Processing of Personal Data. This includes:

☐ The Processor restricts access to facilities containing information systems for the Processing of Personal Data to authorised staff by checking their IDs.

☐ The premises of the Processor are monitored around the clock by a security service through video surveillance or comparable methods at all access points.

☐ The Processor makes use of appropriate security measures to protect against loss of data due to disruptions such as power failure.

5.3 System access control

The Processor takes measures to prevent the data processing systems from being used by unauthorised persons. This includes:

☐ The Processor maintains and updates a list of all authorised users who have access to Personal Data.

☐ The Processor removes the access of users who are no longer employed by the Processor or who have changed their roles.

5.4 Data access control

☐ The Processor ensures that the IT systems used for data processing only grant authorised users the limited access as specified by their individual access rights. This includes:

- The rights of employees to access personal data is limited to the minimum level necessary for their work tasks.

- Personal Data may only be printed in physically secure areas monitored by the Processor and may only be disclosed to employees who need to know about it.

5.5 Monitoring tasks/contracts

The Processor ensures that the Personal Data are processed in accordance with the Controller's instructions. This includes:

☐ Logging of all activities in the area of data processing; this also includes unsuccessful access attempts or authorisation changes;

☐ Regularly checking systems for information security incidents.

5.6 Availability

The Processor ensures that Personal Data cannot be accidentally lost or destroyed. This includes:

☐ Introducing/providing business continuity plans and tests.

☐ Using regular back-up processes and other measures and testing them regularly to enable rapid restoration of systems critical to operations and data when needed.

☐ Using uninterruptible power supplies (for example: UPS, batteries, generators) to ensure the power supply to data centres.

☐ Provision of sufficient data storage capacities.

☐ Regular testing of emergency processes and systems.

5.7 Data separation

The Processor will ensure that data collected for different purposes is Processed separately. This includes the use of technical options (for example client-friendly or separate system landscapes) to separate the Customers' personal data.

5.8 Workplace security

The Processor will take the following measures to guarantee security of all workplaces which are used for access to systems of the Controller to process Personal Data:

☐ a password-protected keyboard lock/screen lock which is activated automatically after a certain period of inactivity (at the latest after 30 minutes).

☐ antivirus and desktop firewall programs will be installed.

☐ immediate installation of safety patches

☐ use of secure passwords