**DATA PROTECTION AGREEMENT**

This Data Protection Agreement ("**Agreement**") is effective as of [date] (the “**Agreement Effective Date**”) by and between [insert Processor’s name] **(**"**Supplier**"**)**;and (ii) [insert Controller’s name] ("**Customer**"). The Agreement forms a part of the Master Services Agreement or any other agreement entered into between Supplier and Customer (“**Underlying Agreement**”). In the event of a conflict between this Agreement and the Underlying Agreement, this Agreement shall control.

# **Definitions**

## In this Agreement, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

### "**Authorised Subprocessors**" means (a) those Subprocessors set out in **Annex 3 Processing Locations and Authorized Subprocessors)**; and (b) any additional Subprocessors consented to in writing by the Customer in accordance with section 5.1;

### "**Process/Processing**", "**Controller**", "**Processor**", "**Data Subject**", **"Personal Data", "Personal Data Breach"** and "**Special Categories of Personal Data**", or equivalent terms, shall have the meaning ascribed to them in Data Protection Laws;

### “**CCPA**” means the California Consumer Privacy Act of 2018, as amended from time to time, including through the California Privacy Rights Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

### "**Data Protection Laws**" means any laws, rules or regulations applicable to the Processing of Personal Data for the performance of the Agreement, including, without limitation, the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), Swiss Data Protection Law, the UK GDPR, the CCPA, and any other applicable national, federal, state, or local data protection or privacy law, together with all laws implementing or supplementing the same;

### "**EEA**" means the European Economic Area;

### "**Customer Personal Data**" means the data described in **Annex 1 (Details of Processing of Customer Data)** and any other Personal Data Processed by Supplier or any Supplier affiliate on behalf of the Customer or any Customer affiliate pursuant to or in connection with the Agreement;

### "**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of Personal Data to Processors established in third countries, as approved by the European Commission in Decision 2021/914/EC, module 2 (transfers Controller-to-Processor), or any set of clauses approved by the European Commission which amends, replaces or supersedes these;

### "**Subprocessor**" means any Processor (including any third party and any Supplier Affiliate) appointed by Supplier to Process Customer Personal Data on behalf of the Customer or any Customer affiliate;

### "**Supervisory Authority**" means (a) an independent public authority which is established by a Member State pursuant to Article 51 GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws;

### “**Swiss Addendum**” means the Swiss Addendum to the Standard Contractual Clauses in **Annex 4 (Swiss Addendum)**;

### “**Swiss Data Protection Law**” means the national legislation of the Swiss Confederation on the protection of Data Subjects with regard to the Processing of Personal Data and on the free movement of such data and other data protection or privacy legislation in force from time to time in the Swiss Confederation;

### “**UK Addendum**” means the United Kingdom addendum to the Standard Contractual Clauses adopted by the United Kingdom Information Commissioner’s Office under section 119A of the Data Protection Act 2018, or any set of clauses adopted by the UK Information Commissioner’s Office which amends, replaces or supersedes these;

### “**UK International Data Transfer Agreement**” means the United Kingdom standard international data transfer agreement adopted by the United Kingdom Information Commissioner’s Office under section 119A of the Data Protection Act 2018, or any set of clauses adopted by the UK Information Commissioner’s Office which amends, replaces or supersedes these; and

### “**UK GDPR**” means the applied GDPR, as that term is defined in section 3 of the Data Protection Act 2018 (UK).

# **Processing of the Customer Personal Data**

## Supplier shall only Process the types of Customer Personal Data relating to the categories of Data Subjects for the purposes of the Agreement and for the limited and specific purposes set out in **Annex 1 (Details of Processing of Customer Data)** to this Agreement and shall not Process, retain, use, sell, share, or combine the Customer Personal Data, nor disclose or permit the disclosure of the Customer Personal Data to any third party, for any other purpose outside the direct business relationship with the Customer other than in accordance with the Customer’s documented instructions (whether in the Agreement or otherwise), unless such Processing is required by applicable laws, as the case may be, to which Supplier is subject, in which case Supplier shall to the extent permitted by such law inform the Customer of that legal requirement before Processing that Personal Data. Supplier shall immediately inform the Customer if, in its opinion, an instruction of the Customer infringes Data Protection Law, or if Supplier can no longer meet its obligations under Data Protection Law. The Customer maintains the right, upon notice, to take reasonable and appropriate steps to stop and remediate Supplier’s unauthorized Processing of Personal Data.

## Supplier shall assist Customer in ensuring compliance with the obligations pursuant to Data Protection Laws, including as applicable [Articles 32](https://www.privacy-regulation.eu/en/32.htm) to 36 of the GDPR, UK GDPR, or similar Data Protection Laws, taking into account the nature of Processing and the information available to Supplier. Supplier shall comply with all Data Protection Laws.

## For the purposes set out in Section 2.1 above, the Customer hereby instructs Supplier to transfer Customer Personal Data to the recipients in the Third Countries listed in **Annex 3 (Processing Locations and Authorized Subprocessors) (**always provided that Supplier shall comply with **Section 5 (Subprocessing)** and **Section 11 (International Transfers of Customer Personal Data)**.

# **Supplier Personnel**

## Supplier shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to access the relevant Customer Personal Data, as strictly necessary for the purposes set out in section 2.1 above in the context of that individual's duties to Supplier, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

# **Security**

## Taking 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, Supplier shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

## Without limitation to section 4.1, Supplier shall implement and maintain each of the technical and organisational measures listed in **Annex 2 (Technical and Organisational Measures)**.

# **Subprocessing**

## Subject to section 5.2, Supplier shall not engage any Subprocessors to Process Customer Personal Data other than with the prior written consent of the Customer, which the Customer may refuse in its absolute discretion. Supplier shall include terms in the contract between Supplier and each Subprocessor which are the same as those set out in this Agreement. Upon request, Supplier shall provide a copy of its agreements with Subprocessors to the Customer for its review.

## As at the Agreement Effective Date, the Customer hereby authorises Supplier to engage those Subprocessors set out in **Annex 3 (Processing Locations and Authorized Subprocessors)**.

# **Data Subject Rights**

## Supplier shall promptly notify the Customer if it receives a request from a Data Subject under any Data Protection Laws in respect of Customer Personal Data.

## Supplier shall co‑operate as requested by the Customer to enable the Customer to comply with any exercise of rights by a Data Subject under any Data Protection Laws in respect of Customer Personal Data and comply with any assessment, enquiry, notice or investigation under any Data Protection Laws in respect of Customer Personal Data or this Agreement, where applicable, providing such assistance as is reasonably requested by the Customer to enable the Customer to comply with the relevant request within the timescales prescribed by the Data Protection Laws.

# **Personal Data Breach**

## Supplier shall notify the Customer promptly, and in any case within twenty-four (24) hours, upon becoming aware of or reasonably suspecting a Personal Data Breach providing the Customer with sufficient information which allows the Customer to meet any obligations to report a Personal Data Breach under the Data Protection Laws.

## Supplier shall co-operate with the Customer and take such reasonable commercial steps as are directed by the Customer to assist in the investigation, mitigation and remediation of each Personal Data Breach.

# **Data Protection Impact Assessment and Prior Consultation**

## Supplier shall provide reasonable assistance to the Customer with any data protection impact assessments which are required under Data Protection Laws and with any prior consultations to any supervisory authority of the Customer or any Customer affiliate which are required under Data Protection Laws, in each case solely in relation to Processing of Customer Personal Data by Supplier on behalf of the Customer and taking into account the nature of the Processing and information available to Supplier.

# **Deletion or Return of Customer Personal Data**

## Supplier shall promptly and in any event within 90 (ninety) calendar days of the earlier of: (i) cessation of Processing of Customer Personal Data by Supplier; or (ii) termination of the Agreement, at the choice of the Customer (such choice to be notified to Supplier in writing) either:

### return a complete copy of all Customer Personal Data to the Customer by secure file transfer in such format as notified by the Customer to the Supplier and securely wipe all other copies of Customer Personal Data Processed by Supplier or any Authorised Subprocessor; or

### securely wipe all copies of Customer Personal Data Processed by Supplier or any Authorised Subprocessor,

### and in each case provide written certification to the Customer that it has complied fully with this Section.

# **Audit rights**

## Supplier shall make available to Customer all information necessary to demonstrate Supplier’s compliance with the obligations of Supplier set forth in this Agreement, and grants Customer the right to take reasonable and appropriate steps to ensure such compliance, including by allowing for and contributing to audits, including inspections, conducted by Customer or another auditor mandated by the Customer.

# **International Transfers of Customer Personal Data**

## Supplier shall not Process the Customer Personal Data nor permit any Authorised Subprocessor to Process the Customer Personal Data in a country that does not provide for an adequate level of data protection in accordance with Applicable Data Protection Laws (a “**Restricted Country**”), other than in respect of those recipients in Restricted Countries (if any) listed in **Annex 3 (Processing Locations and Authorized Subprocessors)**, unless authorised in writing by the Customer in advance.

## Supplier or Subprocessor shall inform Customer if they are no longer able to comply with applicable Data Protection Laws or this Agreement.

## In those jurisdictions that adopt standardized data transfer clauses for legitimizing international transfers between Controllers and Processors, these clauses shall be understood as being incorporated into this Agreement by reference and the Parties shall comply with their obligations in relation to transfers of Customer Personal Data (for clarity, the standard transfer clauses are deemed completed by **Annex 1** and **Annex 3: Processing Locations and Authorized Subprocessors)**. In the event of any conflict or inconsistency between the standard transfer clauses, if applicable, and this Agreement, the clauses shall prevail. For transfers subject to the following Data Protection Laws, the following standard transfer clauses apply:

### for transfer of Personal Data subject to the GDPR, the parties agree to abide by the Standard Contractual Clauses;

### for transfer of Personal Data subject to the GDPR and the UK GDPR, the parties agreed to abide by the Standard Contractual Clauses and the UK Addendum;

### for transfers of Personal Data only subject to the UK GDPR, the parties agree to abide by the UK International Data Transfer Agreement;

### for transfer of Personal Data subject to Swiss Data Protection Law, the parties agree to abide by the Standard Contractual Clauses amended in accordance with the Swiss Addendum in Annex 4.

## When requested by the Customer, Supplier shall promptly enter into (or procure that any relevant Subprocessor of Supplier enters into) an agreement with the Customer or a Customer affiliate as Data Protection Laws might require, in respect of any Processing of Customer Personal Data in a Restricted Country, which terms shall take precedence over those in this Agreement.

# **Indemnification and Liability**

## Notwithstanding any other provision of the Underlying Agreement, a violation of this Agreement by Supplier and Supplier’s indemnification, defense and hold harmless obligations below are not subject to any limitation on the type or amount of Supplier’s liability or any other limitation on Supplier’s liability. Supplier shall indemnify, defend and hold Customer and its affiliates and its and their respective directors, officers, representatives, agents, successors and assigns harmless from and against any and all settlements, judgments, awards, fines, penalties, sanctions, interest, liabilities, losses, costs, damages and expenses, including, without limitation, reasonable attorneys’ fees and disbursements and court costs, arising from or related to Supplier’s violation of this Agreement.

# **General Terms**

## The parties agree that this Agreement shall terminate automatically upon termination of the Underlying Agreement or expiry or termination of all service contracts entered into by Supplier with the Customer pursuant to the Agreement, whichever is later. Any obligation imposed on Supplier under this Agreement in relation to the Processing of Personal Data shall survive any termination or expiration of this Agreement. The governing law and competent jurisdiction of this Agreement is the governing law of the Underlying Agreement.

IN WITNESS WHEREOF, this Agreement is entered into and becomes a binding part of the Underlying Agreement with effect from the Agreement Effective Date first set out above.

|  |  |
| --- | --- |
| **Customer:**Signature | **Supplier:**Signature |
| Name and Title | Name and Title |
| Date | Date |

ANNEX 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

* 1. **LIST OF PARTIES**

**Data exporter(s):** [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: …

Address: …

Contact person’s name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Role: Controller

2. [Add additional lines if necessary, or delete]

**Data importer(s):** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: …

Address: …

Contact person’s name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Role: Processor

2. [Add additional lines if necessary, or delete]

* 1. **DESCRIPTION OF TRANSFER**

*Categories of Data Subjects whose Personal Data is transferred*

*………………………..*

*Categories of Personal Data transferred*

*………………………..*

*Sensitive Personal Data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the Personal Data, restrictions for onward transfers or additional security measures.*

*………………………..*

*The frequency of the transfer (e.g. whether the Personal Data is transferred on a one-off or continuous basis).*

*…………………………*

*Nature of the Processing*

*…………………………*

*Purpose(s) of the Personal Data transfer and further Processing*

*………………………..*

*The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period*

*……………………..*

*Authorization to engage Subprocessors under the standard transfer clauses referred to in Clause 11.3 of the Agreement*

 [Specify time period to submit the authorization or notify changes of Subprocessors]

* 1. **COMPETENT SUPERVISORY AUTHORITY & CHOICE OF LAW AND FORUM**

*Identify the competent supervisory authority/ies in accordance with the standard transfer clauses referred to in Clause 11.3 of the Agreement*

*………………………..*

*Identify the governing law of the standard transfer clauses referred to in Clause 11.3 of the Agreement*

*………………………….*

*Identify the choice of forum and jurisdiction of the standard transfer clauses referred to in Clause 11.3 of the Agreement*

*………………………….*

****ANNEX 2: TECHNICAL AND ORGANISATIONAL MEASURES****

In addition to any measures already agreed to by the Supplier, the Supplier undertakes to institute and maintain the following data protection measures:

* To the extent applicable, Supplier shall comply with all Payment Card Industry Data Security Standard (PCI-DSS) requirements.
* Supplier will comply with all applicable country-specific information security laws, including, to the extent applicable, the technical and organisational security measures specified in Title V, Articles 31 et seq. implemented by Decree no. 196 dated 30 June 2003 (with regard to Italy) and Articles 36-39a of the Polish Act on Personal Data Protection of 29 August 1997 (consolidated text: Journal of Laws of 2014, No 1182).

In addition, Suppler shall comply with the following:

1. Access control of persons

The Supplier shall implement suitable measures in order to prevent unauthorized persons from gaining access to the Customer Personal Data Processing equipment until the Personal Data transferred by the Controller are Processed.

This shall be accomplished by:

 Establishing access authorizations for employees and third parties, including the respective documentations;

 Code card passes;

 Restrictions on keys;

 Regulations for third parties;

 Regulations on key codes;

 Identification of the persons having access authority;

 Security alarm system or other appropriate security measures even after the working time;

 Securing the decentralized Customer Personal Data Processing equipment and personal computers;

 Protection and restriction of access path.

1. Access control to Personal Data

The Supplier commits that the persons entitled to use the Customer Personal Data Processing system are only able to access the Personal Data within the scope and to the extent covered by the respective access permission (authorization).

This shall be accomplished by:

 Locking of terminals;

 Allocation of individual terminals and/or terminal user and identification characteristics exclusive to specific functions;

 Functional and/or time restricted use of terminals and/or terminal users and identification characteristics;

 Regulations for user authorization;

 Obligation to comply with data secrecy;

 User codes for Personal Data and programs;

 Coding routines for files;

 Differentiated access regulations (e.g., partial blocking);

 Regulations for the organisation of files;

 Logging and analysis of use of the files;

 Special control regarding the application of help programs as far as they are able to evade security measures;

 Controlled destruction of data media;

 Work instructions for templates for the registration of Personal Data;

 Checking, adjustment and controlling systems;

 Processes for the checking and release of programs.

1. User Control

The Supplier shall implement suitable measures to prevent its Customer Personal Data Processing systems from being used by unauthorized persons by means of data transmission equipment. In addition, the Supplier shall implement suitable measures to prevent unauthorized reading, copying, alteration or removal of the data media, unauthorized input into memory, reading, alteration or deletion of the stored Personal Data.

This shall be accomplished by:

 Authorization concept;

 Terminal with access user key;

 Identification of the terminal and / or the terminal user to the system of the Supplier;

 Automatic turn-off of the user ID when several erroneous passwords where entered;

 Log file of events (monitoring of break-in attempts);

 Issuing and safeguarding the identification codes;

 Dedication of individual terminals and/or terminal users;

 Identification characteristics exclusive to specific functions;

 Authentication of the authorized personnel;

 Protective measures for the data input into memory as well as for the reading, blocking and deletion of stored Personal Data;

 Use of state-of-the-art encryption for critical security files;

 Specific access rules for procedures, control cards, process control methods, program cataloguing authorization;

 Guidelines for data file organisation;

 Keeping records of data file use;

 Separation of production and test environment for libraries and data files;

 Providing that entries to Customer Personal Data Processing facilities (rooms, housing, computer hardware and related equipment) are capable of being locked;

 Automatic log-off of user IDs that have not been used for a substantial period of time;

 Designating the areas in which data media may / must be located;

 Designating the persons in such areas for authorized remove of data media;

 Controlling the removal of data media;

 Securing the areas in which data media are located;

 Release of data media only to authorized persons;

 Control of files, controlled and documented destruction of data media;

 Policies controlling the production of backup copies.

1. Transmission control

The Supplier shall be obliged to enable the verification and tracing of the locations/destinations to which the Data Subject’s Personal Data are transferred by the utilization of the Supplier’s data communication equipment/devices.

This shall be accomplished by:

 Authentication of the authorized personal;

 In-house verification requirements (four-eye principle);

 Designating the areas in which data media may / must be located;

 Controlling the removal of data media;

 Designating the persons in such areas who are authorized to remove data media;

 Control of files;

 Locking of confidential data media;

 Security lockers;

 Prohibition of taking bags etc. within the secure area;

 Control of destruction of data media;

 Policies controlling the production of backup copies;

 Documentation of the transfer programs;

 Documentation of the retrieval and transmission programs;

 Documentation of the remote locations/destinations to which a transmission is intended and the transmissions path (logical path);

 Authorization policy;

 State-of-the-art encryption of the Data for online transmission or transport by means of data carries (tapes and cartouches);

 Monitoring of the completeness and correctness of the transfer of Data (end to end check);

 State-of-the-art encryption;

 Courier services, personal pickup, accomplishing of the transport;

 Control of plausibility;

 Control of completeness and correctness;

 Deletion of remaining Personal Data before change of data media.

1. Input Control

The Supplier shall provide for the retroactive ability to review and determine the time and the point of the Data Subject’s Personal Data entry into the Supplier’s Customer Personal Data Processing system.

This shall be accomplished by:

 Proof of Supplier’s organisation of the input authorization;

 Electronic recording of entries;

 Electronic recording of Personal Data Processing, in particular usage of Data.

1. Organisation control

The Supplier shall maintain its internal organisation in a manner that meets the requirements of this Agreement.

This shall be accomplished by:

 Internal Personal Data Processing policies and procedures, guidelines, work instructions, process descriptions and regulations for programming, testing and release, insofar as they relate to the Personal Data transferred by the Controller;

 Formulation of a data security concept;

 Industry standard system and program examination;

 Formulation of an emergency plan (backup contingency plan).

1. Instructional control

The Personal Data transferred by the Controller to the Supplier may only be Processed in accordance with the instructions of the Controller.

This shall be accomplished by:

 Binding policies and procedures for the Supplier’s employees;

 Upon request, access will be granted to those of the Controller’s employees and agents who are responsible for monitoring the Supplier’s compliance with this Agreement.

8. Control of separation of Personal Data

 The Supplier shall implement suitable measures to allow the separate Processing of Personal Data which have been collected for different purposes.

This shall be accomplished by:

 Storage of the Personal Data in separated data collectors (physical separation);

 Authorization policy (logical separation);

 Separation of the Personal Data, which have been stored under an alias (pseudonym) from the original Personal Data.

**ANNEX 3: PROCESSING LOCATIONS AND AUTHORIZED SUBPROCESSORS**

**[***Include details of (i) all service locations of the Supplier and each Subprocessor, including those within the EEA and outside of the EEA; (ii) full legal name of each recipient entity to whom data will be transferred, including Subprocessors that are affiliates of the Supplier and any third party Subprocessors; (iii) details of the processing to be undertaken by each entity.***]**

The controller has authorised the use of the following Subprocessors:

1. Name: …

Address: …

Contact person’s name, position and contact details: …

Description of Processing (including a clear delimitation of responsibilities in case several Subprocessors are authorised):

ANNEX 4: SWISS ADDENDUM

For Transfers of Personal Data governed by the Swiss Data Protection Law, the Standard Contractual Clauses shall be amended in accordance with the statement of the Swiss Federal Data Protection and Information Commissioner (“**FDPIC**”) of August 27, 2021. In particular:

1. The FDPIC shall be the competent supervisory authority (Clause 13);
2. The law of the country specified in the Standard Contractual Clauses shall be the governing law (Clause 17);
3. The courts of the country specified in the Standard Contractual Clauses shall be the choice of forum (Clause 18), but this shall not exclude Data Subjects in Switzerland from the possibility of bringing a claim in their place of habitual residence in Switzerland, in accordance with Clause 18(c); and
4. The Standard Contractual Clauses shall protect the data of legal entities in Switzerland until the entry into force of the revised Swiss Data Protection Law.