Version: [2024-06-05]

Annex 5: Data Processing Addendum

This data processing agreement (the ”**Data Processing Addendum**”) forms an integral part of the Service Terms and shall be entered into between us when personal data is processed by us in connection with providing the Services to you. For the purposes of this Data Processing Addendum, the Customer is the “**Data Controller**”, and we are the “**Data Processor**” processing personal data on behalf of the Data Controller.

1. Background

This Data Processing Addendum is required by law.

1.1 Data Protection Regulations stipulate that Processing of Personal Data by a data processor on behalf of a data controller shall be governed by a contract. The parties have entered into the Data Processing Addendum in order to comply with the requirements set out in the Data Protection Regulations.

1.2 This Data Processing Addendum is applicable to the extent that the Data Processor Processes Personal Data on behalf of the Data Controller but only covers the Processing of Personal Data performed in accordance with the Data Controller’s documented instructions in the Data Processing Addendum (including its appendices). Any other form of Processing is not covered. This Data Processing Addendum supersedes previously entered into agreements as well as previous instructions relating to the Processing of Personal Data.

2. Definitions

2.1 In the Data Processing Addendum:

“Data Protection Regulations” means any and all data protection laws and regulations applicable from time to time to the Processing of Personal Data under the Data Processing Addendum (including but not limited to the Swedish Act on complementary provisions to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (2018:218), and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (“**General Data Protection Regulation”**)) as interpreted from time to time by the Court of Justice of the European Union or other court of law that is competent to establish a precedent for such data protection laws.

“**Sub-processor**” Any data processor engaged by the Data Processor for the purpose of Processing the Personal Data.

2.2 Other capitalized terms and expressions in the Data Processing Addendum, which are not defined in Section 2 shall have the same meaning as in the Service Terms or otherwise defined in the Data Processing Addendum. Other terms and expressions of the Data Processing Addendum shall be interpreted in accordance with the General Data Protection Regulation.

3. Processing of Personal Data

We will Process the Personal Data in accordance with your documented instructions and as legally required.

3.1 The Data Controller takes full responsibility to ensure that the Processing of Personal Data and any instructions relating thereto is in compliance with Data Protection Regulations applicable from time to time, including obtaining necessary licenses, permits and approvals for the Processing. The Data Controller is further responsible for ensuring that there is a valid legal basis under article 6 of the General Data Protection Regulation for the Processing of all Personal Data performed by the Data Processor on behalf of the Data Controller.

3.2 The Data Processor shall only Process Personal Data in accordance with the Data Controller’s documented instructions as set out in **Schedule 1**, including transfer of Personal Data to third countries or an international organization, unless the Data Processor has an obligation under EU law (including the laws of its member states) to Process Personal Data. In such case, the Data Processor shall inform the Data Controller of the legal requirement before the Processing is initiated, provided that this is in accordance with applicable laws.

3.3 Schedule 1 of the Data Processing Addendum stipulates the (i) types of Personal Data Processed under the Data Processing Addendum, (ii) categories of Data Subjects that the Personal Data concern, and (iii) nature and purpose for the Processing of Personal Data.

3.4 This Data Processing Addendum, including Schedule 1, constitutes the Data Controller’s entire instructions to the Data Processor for the Processing of Personal Data under the Data Processing Addendum.

3.5 The Data Processor shall immediately inform the Data Controller if the Data Processor considers that all or part of the Data Controller’s instructions are in violation of Data Protection Regulations. The Data Processor shall not implement such instruction until the Data Controller has confirmed that the implementation of the instruction is lawful.

3.6 The Data Processor shall Process the Personal Data for the time necessary in order to fulfil its obligations under the Service Terms.

3.7 The Data Processor shall ensure that persons for whom the Data Processor is responsible and who Process Personal Data under the Data Processing Addendum have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.8 Taking into account the nature of the Processing, the Data Processor shall assist the Data Controller with appropriate technical and organizational measures, insofar as this is possible and to a reasonable extent, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the Data Subjects' rights under the Data Protection Regulations.

3.9 Taking into account the nature of the Processing and the information available to the Data Processor, the Data Processor shall assist the Data Controller in ensuring compliance with the Data Controller's obligations pursuant to Data Protection Regulations, including (where applicable) its obligations to (i) implement appropriate technical and organizational measures, (ii) notify Personal Data Breaches to the supervisory authority, (iii) inform Data Subjects of Personal Data Breaches, (iv) carry out data protection impact assessments, and (v) carry out prior consultation with competent supervisory authorities before Processing.

3.10 The Data Processor shall, at the choice of the Data Controller, delete or return the Personal Data to the Data Controller at the end of the term of the Data Processing Addendum, and delete existing copies unless EU law (including the laws of its member states) requires storage of the Personal Data. If requested by the Data Controller, the Data Processor shall provide written notice confirming the return or deletion of the Personal Data. The Data Processor's responsibility under this Section 3.10 only concerns deletion and return of Personal Data pursuant to Data Protection Regulations.

4. Security of Processing

We will keep the Processing of the Personal Data secure and thereby protect the privacy of the Data Subjects.

4.1 The Data Processor shall implement appropriate technical and organizational security measures in accordance with Data Protection Regulations to ensure a level of security appropriate to the risk and, when appropriate:

(a) pseudonymisation and encryption of Personal Data;

(b) ensure that there is a procedure for regular testing, investigation and evaluation of the efficiency of the technical and organizational security measures to ensure the security of the Processing;

(c) maintain and update logs regarding Personal Data, establish and maintain an IT-security policy, maintain a secure IT-environment as well as establishing and maintaining physical security measures and routines; and

(d) inform the Data Controller of any attempt at or completion of unauthorized access to Personal Data (including loss or change of Personal Data).

4.2 The Data Processor is only responsible for implementing appropriate technical and organizational security measures in accordance with Section 4.1 that are within the actual control of the Data Processor.

4.3 The Data Processor shall notify the Data Controller without undue delay after the Data Processor becoming aware of a Personal Data Breach (as defined in Data Protection Regulations). Such notification shall, taking into account the nature of the Processing and the information available to the Data Processor:

(a) describe the nature of the Personal Data Breach and, insofar as this is possible, the categories and approximate number of Data Subjects and Personal Data that are concerned;

(b) describe the likely consequences of the Personal Data Breach; and

(c) describe the measures that have been taken or proposed to be taken to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

If and to the extent it is not possible for the Data Processor to provide all of the information at the same time, the information may be provided in several phases without undue delay.

4.4 If the Data Controller does not notify the Data Subjects of a Personal Data Breach, thereby failing to comply with Data Protection Regulations, and a competent supervisory authority subsequently orders the Data Processor to remedy such failure, the Data Controller shall compensate the Data Processor for any costs related to complying with such supervisory authority's decision.

5. Audit (inspection)

To ensure that we are in compliance with this Data Processing Addendum, you have the right to conduct audits.

5.1 The Data Processor shall make all information available to the Data Controller that is necessary to demonstrate compliance with the obligations set out in the Data Processing Addendum. The Data Controller, or any auditor mandated by the Data Controller, is entitled to conduct audits, including inspections, of the Data Processor's compliance with the Data Processing Addendum one time per year during normal business hours. Such audit shall be preceded by at least thirty (30) days' prior written notice from the Data Controller, in which the content and the extent of the audit shall be specified. The purpose of such audits shall be to verify the Data Processor's compliance with the obligations set out in the Data Processing Addendum. The content and extent of an audit may not exceed what is necessary to achieve the purpose of the audit. Unless the parties have agreed otherwise in writing, the inspection may only be conducted if an audit in accordance with Data Protection Regulations cannot be completed through the provision of information by the Data Processor. Any costs relating to an audit shall be at the Data Controller's expense. The Data Processor's reasonable costs relating to such audit Data Processor may also be charged to the Data Controller.

5.2 An audit in accordance with Section 5.1 requires that the Data Controller, or the auditor appointed by the Data Controller, has agreed on necessary confidentiality undertakings and complies with the security measures of the Data Processor at the site where the audit shall be performed. Furthermore, the audit shall be carried out without unreasonably disturbing the Data Processor's business or risking the protection of third parties' information. Any information collected in connection with the audit shall be deleted immediately after the completion of the audit or as soon as the information is no longer required for achieving the purpose of the audit.

6. Sub-processors

We are allowed to get help to Process the Personal Data.

6.1 The Data Controller hereby provide the Data Processor with a general authorization to engage Sub-processors for the Processing of Personal Data.

6.2 The Data Processor shall inform the Data Controller of any plans to engage new Sub-processors or replace Sub-processors in order for the Data Controller to be able to object to such changes. The Data Controller shall object to such new or replaced Sub-processors within five (5) business days from the day of the Data Processor's notice concerning the new or replaced Sub-processor. The Data Controller shall not object to engagement of new Sub-processors or replacement of Sub-processors, if the new Sub-processor has sufficiently undertaken to implement technical and organizational security measures in compliance with Data Protection Regulations and ensures the safeguarding of Data Subjects' rights. If the Data Controller has not objected to the new or replaced Sub-processor within the timeframe, the Data Controller shall be considered to have approved the Sub-processor. If the Data Controller objects to a new Sub-processor within the timeframe, the Data Processor shall be entitled to terminate the Service Terms to take effect immediately or as otherwise agreed between the parties.

6.3 If the Data Processor engages a Sub-processor for Processing Personal Data on behalf of the Data Controller, equivalent data protection obligations as set out in the Data Processing Addendum shall be imposed on that Sub-processor by way of a contract. The Data Processor shall at all times remain fully responsible for all obligations, acts and omissions of any Sub-processor to the same extent as if performed or not performed by the Data Processor itself.

7. Processing of Personal Data in countries outside of the EU/EEA

Any Processing outside the EU/EEA must in accordance with the law.

7.1 Unless otherwise agreed to in Schedule 1, the Data Processor shall not transfer and shall ensure that any Sub-processors do not transfer, any Personal Data to a country outside of the EU/EEA.

7.2 If the Parties have agreed that Personal Data may be transferred to a country outside of the EU/EEA, the Data Processor shall ensure that appropriate safeguards are provided in accordance with applicable Data Protection Regulations. Such appropriate safeguards may include, but are not limited to, the Data Processor (i) entering into a contract with a Sub-processor based upon the EU Commission's standard contractual clauses (SCC) for the transfer of Personal Data to a country outside the EU/EEA; or (ii) adhering to approved binding corporate rules (BCR). A transfer of Personal Data to a country outside the EU/EEA may also be based upon a valid adequacy decision by the EU Commission.

7.3 The Data Processor may transfer Personal Data outside of the EU/EEA if the Data Processor has an obligation to do so under EU law or the laws of its member states, and if the Data Processor has informed the Data Controller of the legal requirement before the transfer is made, unless such laws prohibit such information on important grounds of public interest.

7.4 To the extent the Data Controller is a recipient of Personal Data in a country outside of EU/EEA that is not recognized as providing an adequate level of protection for Personal Data (as set forth in the General Data Protection Regulation), the Data Controller and the Data Processor agree to abide by and process Personal Data in compliance with Schedule 2 (Standard Contractual Clauses). In case of conflict between any provisions of this Data Processing Addendum and Schedule 2, Schedule 2 shall take precedence.

8. Confidentiality

Both parties promise to keep the Processing of Personal Data confidential.

The Data Processor undertakes not to disclose any information regarding the Processing of Personal Data under the Data Processing Addendum to any third parties or in any other way disclose any other information received as a result of the Data Processing Addendum. The obligation of confidentiality does not apply to information to sub-processors according to Section 6 and/or information that the Data Processor is obliged to disclose according to EU Regulations (including the laws of its member states) or decisions of authorities. In addition to this Section 8, any undertakings as to confidentiality in the Service Terms shall also be applicable. When the Data Processing Addendum terminates, regardless of reason, this Section 8 will continue to be binding for both parties.

9. Liability

Our liability is the same as in the Service Terms, but any limitation of liability in this Data Processing Addendum does not apply to administrative fines imposed by the supervisory authority.

9.1 The Data Processor is responsible for direct damage resulting from the Data Processor's Processing of Personal Data outside of the scope of or in violation of the Data Controller's lawful instructions in the Data Processing Addendum. Nevertheless, the Data Controller is responsible for all direct or indirect damage caused by Processing of Personal Data under the Data Processing Addendum and in accordance with Schedule 1 that is in breach with Data Protection Regulations. To the extent permitted by applicable laws, the Data Processor's total liability for any damage or loss of any kind (regardless of how it was caused and including any damage or loss caused by negligence) under or in connection with the Data Processing Addendum shall be subject to the limitation of liability in the Service Terms.

9.2 Notwithstanding the above, the Data Controller shall hold the Data Processor harmless if and to the extent the Data Processor is held liable by a Data Subject or other third party (including claims from supervisory authorities) for unauthorized or unlawful Processing of Personal Data, unless such liability has arisen as a consequence of the Data Processor's failure to perform its obligations under the Data Processing Addendum. The Data Controller shall also hold the Data Processor harmless if and to the extent the Data Processor is held liable by a Data Subject or other third party for unauthorized or unlawful Processing of Personal Data if such liability has arisen from the Data Controller's instructions in Schedule 1.

9.3 The limitation of the parties' liability in this Section 9 above does not apply to the administrative fines imposed by the supervisory authority and/or court in accordance with Article 83 of the General Data Protection Regulation. Neither party is entitled to remuneration from the other party for any administrative fines that the party is obliged to pay according to a decision of the supervisory authority and/or court. The parties acknowledge and agree that the parties may become individually liable for administrative penalty fees in accordance with Article 83 of the General Data Protection Regulation.

9.4 This Section 9 shall survive the termination of the Data Processing Addendum, regardless of the reason for termination.

10. General Provisions

Here are some more important details about this Data Processing Addendum.

10.1 This Data Processing Addendum will remain in full force and effect until the Data Processor ceases to Process Personal Data on behalf of the Data Controller according to the terms of the Service Terms.

10.2 Changes and additions to the Data Processing Addendum, including this Section 10.2, must be in writing and duly executed by the parties in order to be binding.

10.3 If the Data Protection Regulations are amended during the term of the Data Processing Addendum, or if a competent supervisory authority issues guidelines, decisions or regulations regarding the application of the Data Protection Regulations which causes the Data Processing Addendum to not meet the requirements of a Data Processing Addendum, or if the Service Terms is amended, the Data Processing Addendum shall be amended to meet such new or additional requirements and/or amendments.

10.4 This Data Processing Addendum contains the entire agreement between the parties with respect to the subject matter hereof, and supersedes all previous and contemporaneous negotiations and understandings between the parties in relation thereto, whether written or oral. In case of any conflict between the Data Processing Addendum and any other agreement between the contracting parties, the Data Processing Addendum shall take precedence. However, the foregoing does not apply to subsequent agreements expressly stated to take precedence over the provisions set out in the Data Processing Addendum. In addition to the Data Processing Addendum, any relevant provisions in the Service Terms shall also be applicable to the Data Processor's Processing of Personal Data. In case of any conflict between the Service Terms and the Data Processing Addendum, the Data Processing Addendum shall take precedence with regard to the Processing of Personal Data.

11. Governing Law and Dispute Resolution

In the unlikely event the parties end up in a legal dispute, the parties agree to resolve it by arbitration subject to confidentiality.

11.1 This Data Processing Addendum shall be applied and interpreted in accordance with the laws of Sweden, excluding its conflict of laws principles providing for the application of the laws of any other jurisdiction.

11.2 Any dispute concerning the interpretation or application of the Data Processing Addendum shall be settled in accordance with the provisions on dispute resolution in the Service Terms.

Schedule 1 – Instruction for Processing of Personal Data

1. Nature and purpose of Processing

The Data Controller instructs the Data Processor to only Process the Personal Data for the purpose of enabling the provision of the Services under the Service Terms, including but not limited to:

(a) Processing the Personal Data as necessary to setup the Data Controllers' access to the Services;

(b) Processing the Personal Data as necessary to facilitate the technical provisioning of Logivity Access, such as by transmitting Personal Data over the network and storing it in required databases;

(c) Processing the Personal Data as necessary to provide features of the Services, including storage of off-chained databases necessary to provide supporting services for quality performance purposes;

(d) Processing the Personal Data as necessary for the purpose of providing and maintaining the Services to the Data Controller in accordance with the Service Terms;

(e) Processing the Personal Data as necessary to offer and provide support services to the Data Controller using the Logivity Connect service under the Service Terms;

(f) Processing the Personal Data as necessary to enable us to provide contact information to and between Logistics Service Providers and the Transport Buyer in connection with a Shipment offered through the Logivity Loadboard;

(g) Processing the Personal Data as necessary for the storage of transportation data when retained for invoicing purposes; and

(h) Processing the Personal Data as necessary to manage authorization, authentication, and scope of access for the Data Controller.

2. Type of Personal Data

The Data Processor will Process the following five types of Personal Data:

(a) **Profile data** – is Personal Data linked to a Data Controller's Logivity-ID and/or Membership, as necessary to build profiles representative of the Data Controller as a Member and is used for identity management, single sign-on, and identity governance. For example, name, professional role, email address and phone number to the representative of the Data Controller.

(b) **Transaction related data** – is Personal Data related to Shipments and other transportation services relating to the Services. For example, name, role, email address and phone number of a contact person of the Data Controller may be filled out in the contact fields of the data structure related to the transaction. Further, hashes of underlying Personal Data are written on the ledger.

(c) **Incidental data** – is Personal Data collected within the transaction. Personal Data may occur if the Data Controller fills out any free text fields relating to a transaction with information containing Personal Data, e.g., contact information. For example, ”Joe is ready to deliver goods; please call him at +46…”. Further, hashes of underlying Personal Data are written on the ledger.

(d) **Technical data and Service data**– is Personal Data relating to the Data Controller's use of the Services, including; (i) technical data such as IP address, for network optimization, maintenance, internal audit and monitoring purposes, and (ii) organizational data such as brand or company name if the Data Controller operates under sole proprietorship.

(e) **Off-chain database data –** is Personal Data relating to organization details which are stored in an off-chain database for maintenance and back-up purposes, including Personal Data regarding the organization administrator person and the organization authorized person connected to the Data Controller's Logivity-ID.

3. Categories of Data Subjects

The Personal Data concern the following categories of Data Subjects:

(a) Representatives of the Data Controller;

(b) Contact persons of the Data Controller, to the extent the Data Controller includes it in connection with using the Services; and

(c) Drivers, carriers and similar data subjects, to the extent the Data Controller specifies this in connection with using the Services.

4. Location of Processing

The Data Processor may Process Personal Data in the following countries:

(a) Any country within the EU/EEA;

(b) Any country outside the EU/EEA provided that the transfer (i) is in compliance with the obligations under this Data Processing Addendum, (ii) permitted under Data Protection Regulations and (iii) necessary in order to facilitate the provision of services provided by the Sub-processors outlined in Section 5 of this Schedule 1 (including the processors of such Sub-processors).

5. Engaged Sub-processors

The Data Processor is engaging the following Sub-processors:

Company name	Company reg. no.	Categories of Personal Data	Purpose of Processing
Oracle Svenska AB	556254-6746	All categories included under Section 1.	Providing hosting infrastructure.

6. Technical and organisational measures to be implemented by the Data Processor

The Data Processor shall:

(a) prevent access by unauthorised persons to data processing equipment with which the Personal Data are Processed and used (equipment access control).

(b) prevent unauthorised persons from using the data processing systems and ensure routines for granting, changing and removal of access to such systems (systems access control).

(c) ensure that those authorised to use a data processing system can access only the data relevant to their authorised access and that Personal Data cannot be read, copied, amended or removed without authorisation during Processing (data access control).

(d) ensure that Personal Data cannot be read, copied, amended or removed without authorisation during their electronic transfer or their transportation or their storage on data media and that it is possible to check and determine at what points transfer of Personal Data by facilities for data transmission is anticipated (transfer control).

(e) ensure that it is possible to check and determine after the event whether and by whom Personal Data have been input or amended in or removed from data processing systems (input control),

(f) ensure that Personal Data can only be Processed in accordance with the Data Controller’s instructions (service control).

(g) ensure that Personal Data are protected against accidental destruction or loss (availability control).

(h) ensure that data gathered for various purposes can be Processed separately (separation control).

Schedule 2 - Standard Contractual Clauses

These Standard Contractual Clauses (processor to controller) as set forth in this Schedule 2 form an integral part of the Data Processing Addendum.

SECTION I

1. Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural per-sons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the legal entity defined in the Service Terms transferring the personal data, as listed in Annex I.A. (hereinafter the "**data exporter**"); and

(ii) the legal entity defined in the Service Terms, any applicable order confirmation, and/or corresponds to the information associated with the user account used to order the Services, receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter the "**data importer**"),

(each a "**Party**" and collectively the "**Parties**") have agreed to these standard contractual clauses ("**Clauses**").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

2. Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

3. Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions: (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7; (ii) Clause 8.1 (b) and Clause 8.3(b); (iii) Clause 9 (omitted); (iv) Clause 12; (v) Clause 13 (omitted); (vi) Clause 15.1(c), (d) and (e); (vii) Clause 16(e); (viii) Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

4. Interpretation

(a) Where these Clauses use terms that are de-fined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

5. Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

6. Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

7. Docking clause

(Omitted)

SECTION II – OBLIGATIONS OF THE PARTIES

8. Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 **Instructions**

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 **Security of processing**

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access ("**personal data breach**"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks in-volved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(a) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data im-porter in addressing the breach.

(b) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 **Documentation and compliance**

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

9. Use of sub-processors

(Not applicable)

10. Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects un-der the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

11. Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

12. Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the da-ta subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

13. Supervision

(Not applicable)

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

14. Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safe-guard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved, and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal da-ta in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data ex-porter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on re-quest.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the con-tract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has rea-son to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify ap-propriate measures (e.g., technical or organisational measures to ensure security and confidentiality) to be adopted by the data export-er and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data ex-porter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

15. Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the da-ta exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information avail-able to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data import-er agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data im-porter under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the mini-mum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

16. Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data im-porter until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the trans-fer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

(d) In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(e) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data im-porter that prohibit the return or deletion of the transferred personal data, the data im-porter warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(f) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

17. Governing law

These Clauses shall be governed by the law as specified in the Service Terms.

18. Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved as specified in the Service Terms.

APPENDIX - ANNEX I

A. LIST OF PARTIES

Data exporter. The name, address and contact information of the data exporter is defined in the Service Terms. The data exporter processes personal data as a data processor in the context of activities relevant for the provision of Services under the Service Terms.

Data importer. The name, address and contact information of the data importer is defined in the Service Terms, any applicable order confirmation, and/or corresponds to the information associated with the user account used to order the Services. The data importer processes personal data as a data controller in the context of activities relevant for the use of Services under the Service Terms.

B. DESCRIPTION OF TRANSFER

The categories of personal data (including sensitive data), categories of data subjects, and as well as the nature and purpose of the processing is defined in the Service Terms.

The personal data is continuously transferred and retained for the duration of the provision of Services under the Service Terms.