FUJITSU

Fujitsu Enterprise Postgres Support Terms and Conditions for Red Hat Marketplace

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SUPPLIER WILL PROVIDE THE SUPPORT SERVICES TO CUSTOMER ONLY IF CUSTOMER FIRST ACCEPT THE TERMS OF THIS AGREEMENT. BY USING THE SOFTWARE, CUSTOMER AGREE TO THESE TERMS.

Supplier will use commercially reasonable efforts to respond to the Support Call from the Pre-Registered Contacts for the Software used according to Customer's environment during the Support Period, provided Customer have fully prepaid the annual subscription fees of applicable the Software as defined in the Fujitsu Annual Subscription Agreement provided separately.

The term "Supplier" hereunder shall mean who sells and provides the Support to Customer.

1 Definitions

1.1. "Documentation" means documentations including Read Me files contained in the Software.

1.2. "Error" shall mean a failure of the Software to materially conform to the specifications as described in the applicable Documentation.

1.3. "Initial Response Time" shall mean the target for the elapsed period measured from the time that Customer raises a Support Call until Supplier provides a response which is Supplier's acknowledgment of a Support Call received from Customer.

1.4. "Pre-Registered Contact" shall mean the designated five persons by Customer to be the primary contact points who will submit a notice of technical incidents from Customer to Supplier.

1.5. "Software" shall mean a software defined in the purchase agreement or purchase order form.

1.6. "Support" shall mean the support service provided by Supplier as more specifically described in Section 2.

1.7. "Support Call" shall mean a notice of technical incidents from the Pre-Registered Contact to Supplier via the designated method to contact including web based support system.

1.8. "Support Period" shall mean the subscription period of applicable Software as defined in Fujitsu Annual Subscription Agreement unless otherwise agreed separately in writing.

1.9. "Target Resolution Time" shall mean the target for Supplier of the time required to provide a documented fix that restores full or near full functionality to Customer. This documented fix includes Workarounds. This time shall not include the time delay arising from the time which Supplier waits for Customer's response.

1.10. "Workaround" is a resolution focusing on operational procedures concerning the use of the Software as a result of which Customer can avoid the adverse effects of an Error in the Software without severely compromising the performance of the Software or the integrity of the system or data which operates in conjunction with the Software.

2 Support

2.1 Support

Supplier will use commercially reasonable efforts to provide the followings for applicable Software as the Support during the Support Days and Hours set forth in 2.4 of Section 2:

- a Response to the Support Call to the Pre-Registered Contact;
- the notifications of patch release, failures and security information;
- upgraded version of the Software upon Customer's request with the conditions defined in Fujitsu Annual Subscription Agreement provided separately.

2.2 Customer's responsibilities

Customer will provide the followings to Supplier before the Support Call or until the Support Call is confirmed as closed:

- identify incidents related to the Software;
- isolate and identify problems;
- provide necessary assistance and information reasonably required to solve problems.

Customer is responsible for ensuring the protection of any data containing sensitive, confidential or personal information, including obscuring the logs or otherwise safeguarding such information prior to sending it to Supplier.

Customer acknowledges that Supplier may provide such information to Supplier's subcontractors to solve such problems.

2.3 Support Exclusions

Supplier will not provide the Support in any of the following circumstances:

- An Error and/or inquiry of hardware, network, cloud platform, equipment or software programs other than the Software.
- An Error and/or inquiry from Open Source Software which is not defined in the Documentation of the Software.
- Customer's failure to comply with operating instructions contained in the Documentation.
- Failure to comply with the terms and conditions defined in Fujitsu Annual Subscription Agreement.
- A modification, enhancement or customization of the Software.
- Any cause or causes beyond the reasonable control of Supplier (e.g. floods, fires, loss of electricity, network or other utilities).
- Errors and/or inquiry related to the Software where the applicable support fee is not paid to Supplier.
- An Error and/or inquiry about installation, configuration, management and operation of Customer's applications
- Any professional service requests including, but not limited to performance tuning, advices on design and assistance to installation.
- APIs interfaces or data formats other than those included with the Software
- The Support through access to customer environments remotely/physically.
- The Support call from other contacts than the Pre-Registered Contacts. Supplier will not provide the Support to other contacts than the Pre-Registered Contacts including, but not limited to, Customer's partner and end customers.

2.4 **Support Level**

	Severity 1	Severity 2	Severity 3	Severity 4
Initial Response Time	1 hour			
Target Resolution Time	24 hours	48 hours	7 days*	Best efforts / Future version of software
Support Hours	24 hours			
Support Days	Sunday to Saturday			
Language	English			

* It excludes December 30th through January 3rd in Japan.

2.5 **Definitions of Severity level**

Severity	Definition
Severity 1 - Critical	In a production environment, after a problem occurred in which the user business is completely stopped (Example: file corruption, system down), the recovery also fails, and the business cannot be resumed because there is no Workaround acceptable to the user.
Severity 2 - High	The business is resumed by a temporary Workaround after a part of the user's business in the production environment is stopped or a problem that causes a serious failure to the user's business occurs. But, troubles occur frequently and the business is greatly affected since an effective Workaround cannot be found.
Severity 3 - Moderate	The user's business may be fully used in production environment. However, a feature does not work.
Severity 4 - Low	Aesthetics or changes for convenience; no functional implications

3 Warranties

Supplier warrants that: the Support will be performed in a professional and workmanlike manner. For any breach of the foregoing warranties, Customer's sole and exclusive remedy, and Supplier's sole and exclusive obligation, will be for Supplier to re-perform the Support as warranted, as applicable. If Supplier is unable to correct such non-conformance in the Support after a reasonable opportunity, Supplier will refund the subscription fees paid for the non-conformance; provided that these remedies are only available if Supplier receives notice of such breach within ten (10) days from the date of delivery of the Support, as applicable.

4 Limitations of Liability.

In no event that Supplier's liability arising under this agreement exceed the amount of subscription fee paid by Customer for the 12 months period immediately preceding the event giving rise to such liability. Supplier will not be liable to Customer for any consequential, incidental, special, indirect, or exemplary damages, including without limitation lost profits, business, contracts, revenue, goodwill, production, anticipated savings, loss of data, or costs of procurement of substitute goods or services, or, for any claim or demand by Customer, however caused and (to the fullest extent permitted by law) under any theory of liability (including negligence) even if Supplier has been advised of the possibility of such damages. Customer acknowledges that the amounts payable hereunder are based in part on these limitations, and further agree that these limitations shall apply notwithstanding any failure of essential purpose of any limited remedy.

5 Personal Data

Personal data provided to Supplier for the purpose of the Support will be processed in accordance with Exhibit A. For the avoidance of doubt, this provision does not exempt Customer from Customer's obligations under the agreements stipulating the details of the Support.

EXHIBIT A

Data Processing Addendum

A. This Data Processing Addendum (the "Data Processing Addendum") is a part of Fujitsu Enterprise Postgres Support Terms and Conditions for Red Hat Marketplace between Supplier and Customer (the "**Agreement**") for the provision of goods and/or services by Supplier or Supplier Processors to Customer.

B. To the extent that the Agreement already contains obligations relating to:

   compliance with laws and change of laws;

   data protection;

   security; and

   confidentiality,

   then this Data Processing Addendum supplements such obligations in the Agreement and does not directly replace or release existing obligations. In the event of a conflict or inconsistency between the terms, the terms of this Data Processing Addendum shall prevail to the extent the conflict relates to the subject matter of this Data Processing Addendum.

C. This Data Processing Addendum sets out how Supplier and the Supplier Processors are to perform their obligations in the context of the Applicable Privacy Law.

Supplier and Customer now agree this Data Processing Addendum as set out above and on the following pages which, along with Schedule 1 and all Appendixes thereto, all form part of and are included in this Data Processing Addendum.

SCHEDULE 1: DATA PROCESSING DESCRIPTION AND APPLICABLE TERMS

DATA PROCESSING DESCRIPTION

Subject matter and duration of processing

Processing of the Processed Personal Data as a direct result of the Agreement and for the duration of Support Period as defined in the Agreement.

Nature and purpose of processing

Processing is for the purposes of Supplier meeting its obligations regarding Support as defined in the Agreement, to Customer under the Agreement and in accordance with the Applicable Law.

Types of Processed Personal Data

Personal data provided by Customer for the purposes of the receipt of goods and/or services in accordance with the Agreement.

Approved Supplier Processors

Customer has consented to Supplier's use of the following Supplier Processors for the purpose of providing the Services and in accordance with this Data Processing Addendum:

Fujitsu Technology Solutions Sp. z o.o.,

Fujitsu Services Limited,

Fujitsu Consulting India Private Limited,

Fujitsu Australia Limited,

K.K. Box Japan,

Box, Inc.

Categories of Data Subjects

Data in respect of individual data subjects provided by Customer or obtained or derived by Supplier pursuant to performance of the Agreement being data in respect of data subjects including:

Customer data subjects including Customers' employees, Customers' representatives

APPLICABLE TERMS

DEFINED TERMS

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control", for the purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Applicable Law" means any and all applicable provisions of statutes, laws, rules, codes, treaties, ordinances, decisions, directions, injunctions or regulations, including from any court or any regulatory or governmental authority in any jurisdiction which is relevant to the Services and/or the Agreement.

"Applicable Privacy Law(s)" means any Applicable Law on or relating to data protection or data privacy as amended or updated from time to time.

"Data Subject" shall have the meaning as defined under Applicable Privacy Law or if there is no such definition, means the identified or identifiable natural person to whom Personal Data relates.

"Personal Data" means any information relating to an identified or identifiable natural person; an identifiable natural person is someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Personal Data Breach" means

i) a data breach as defined in the Applicable Privacy Law (if any); or

ii) if there is no definition in the Applicable Privacy Law, a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Processed Personal Data.

"Processed Personal Data" means Personal Data processed by Supplier and/or any Supplier Processor in the course of i) providing the Services, or ii) otherwise performing obligations under the Agreement.

"Service Recipient" means Customer and/or another person receiving services under the Agreement.

"Services" means the goods or services to be provided under the Agreement.

"Sub-Contractor" means a person (other than an employee) sub-contracted or otherwise used by Supplier (directly or indirectly) to perform services under the Agreement (not necessarily services involving the processing of Personal Data).

"Supplier Processor" means Supplier's Affiliates or Sub-Contractors processing Processed Personal Data in accordance with this Data Processing Addendum.

"Supervisory Authority" means an independent public authority that has jurisdiction over the processing of Personal Data under this Data Processing Addendum or, as the case requires, a government agency or authority that has jurisdiction over the processing of Personal Data under this Data Processing Addendum.

To the extent relevant under Applicable Privacy Law, the terms "processing", "processor" and "controller" shall have the meaning given to them in the Applicable Privacy Law.

1. SUPPLIER OBLIGATIONS

Where the Supplier and/or a Supplier Processor processes Processed Personal Data in the course of providing the Services, or otherwise to perform obligations under the Agreement and/or this Data Processing Addendum for Customer:

1.1 Supplier shall comply with Applicable Privacy Law in relation to the processing of Processed Personal Data;

1.2 the parties acknowledge that, to the extent relevant under the Applicable Privacy Laws, Supplier will act as a processor for Customer as controller;

1.3 Supplier shall align their processing with the Data Processing Description set out in Schedule 1 and any other processing description agreed in writing between the parties which forms part of this Data Processing Addendum;

1.4 Supplier shall only process the Processed Personal Data on the documented instructions of Customer and in accordance with this Data Processing Addendum; and

1.5 Supplier shall ensure that any persons including their employees authorised to process, or otherwise have access to, the Processed Personal Data have committed themselves to confidentiality on appropriate terms and/or are under an appropriate binding legal obligation of confidentiality.

2. CUSTOMER OBLIGATIONS

2.1 Customer warrants, represents and undertakes for itself and for any other Service Recipient that (i) Customer and/or such Service Recipient shall comply in all respects with Applicable Privacy Laws; and (ii) all instructions Customer and/or such Service Recipient gives to Supplier regarding Processed Personal Data shall at all times be in accordance with Applicable Privacy Laws.

2.2 Customer and/or any other Service Recipient is responsible for complying with all obligations under Applicable Privacy Law (including any obligations to give notice to and/or obtain consent from individuals whose Personal Data is processed under the Agreement or this Data Processing Addendum) such that Supplier can lawfully process the Processed Personal Data as contemplated by this Data Processing Addendum.

3. TECHNICAL AND ORGANISATIONAL MEASURES

Supplier shall at all times have in place technical and organisational measures to protect the Processed Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. Such measures shall be appropriate to the risks of varying likelihood and severity to the rights and freedoms of individuals that arise as a result of the processing, taking into account the state of the art, the costs of implementation and the nature, scope, context and purpose of the processing ("**Appropriate**"), including implementing an Appropriate information security program in accordance with the security measures set out in Appendix 1 (Security Requirements).

4. COOPERATION

4.1 Supplier shall give Customer, at Customer's reasonable cost, such co-operation, assistance and information as Customer may reasonably request and Supplier may reasonably be able to provide, taking into account the nature of processing and the

information available to Supplier, and as is necessary to enable Customer to comply with its obligations under Applicable Privacy Laws and co-operate with the Supervisory Authority in relation to the Processed Personal Data, including assisting Customer:

4.1.1 by taking appropriate technical and organisational measures, to respond to requests from Data Subjects for access to or rectification, erasure, portability, or restriction of or objection to processing, of Processed Personal Data; and

4.1.2 in ensuring compliance with Customer's security, data breach notification, impact assessment and Supervisory Authority consultation obligations under Applicable Privacy Laws, taking into account the information available to Supplier.

5. SUBPROCESSING

5.1 Customer agrees that Supplier may disclose, transfer, or make accessible the Processed Personal Data to Supplier Processors for the purpose of providing the Services under the Agreement subject to the following:

5.1.2 Supplier shall maintain a list of Supplier Processors and the processing activities to be performed in connection with such disclosures;

5.1.2 Supplier shall provide Customer with at least 8 working days' prior notice of the addition of any new Supplier Processor to this list and the opportunity to object to such addition; and

5.1.3 if Customer, acting reasonably, makes such an objection on reasonable grounds and Supplier is unable to modify the Services to prevent disclosure of Processed Personal Data to the additional Supplier Processor, Customer and Supplier shall negotiate in good faith to agree an appropriate replacement Supplier Processor.

5.3 Supplier shall ensure that each (if any) Supplier Processor is party to a written contract imposing on it obligations which are (at least) materially equivalent to those imposed on Supplier by this Data Processing Addendum.

5.4 Supplier shall remain responsible for the compliance by any Supplier Processor with the terms of the Applicable Privacy Law and this Data Processing Addendum.

6. DATA SECURITY INCIDENT

6.1 Supplier shall, without undue delay, give written notice to Customer, if it becomes aware of the occurrence of any Personal Data Breach.

6.2 In relation to any Personal Data Breach Supplier shall:

6.2.1 take reasonable steps to identify and mitigate the underlying cause of the Personal Data Breach so as to minimise the risk of its repetition and the occurrence of similar Personal Data Breach;

6.2.2 take such steps as Supplier may consider necessary to mitigate the risk to Data Subjects as a result of the Personal Data Breach; and

6.2.3 on reasonable request from Customer and subject to obligations of confidentiality, make available to Customer information about the Personal Data Breach necessary for Customer to comply with its obligations under Applicable Privacy Law.

7. AUDIT

7.1 Supplier shall make available to Customer all information (including records and written documents) necessary to demonstrate Supplier's compliance with its obligations under Applicable Privacy Law in relation to the Processed Personal Data.

7.2 If Customer is not reasonably satisfied that the information provided to Customer by Supplier reasonably demonstrates Supplier's compliance with its obligations under Applicable Privacy Law in relation to the Processed Personal Data, Supplier shall allow for and contribute to audits, including inspections, conducted by Customer (or its appointed auditor) subject to the following:

7.2.1 Customer shall give Supplier no less than one month prior written notice of any audit or inspection to be conducted and shall ensure that Customer makes (and ensures that each of its appointed auditors makes) reasonable endeavours to avoid causing any material impact on Supplier in the course of such an audit or inspection;

7.2.2 the audit shall only be undertaken inside normal business hours (9am – 5pm on a weekday excluding public holidays);

7.2.3 Customer shall undertake no more than one audit in any calendar year, except for any additional audits or inspections which Customer is required or requested to carry out by Applicable Law or a Supervisory Authority; and

7.2.4 Customer (and its appointed auditors) shall not be authorised to access, copy or otherwise process any other Customer or Supplier data that is not Processed Personal Data.

7.3 Customer shall ensure that before any audit is undertaken the individual conducting the audit has entered into a confidentiality agreement with Supplier and that the individual is only authorised to access documents or areas of Supplier which are necessary to demonstrate compliance with Applicable Privacy Law.]

8. PROCESSING INSTRUCTIONS

8.1 Supplier shall inform Customer (but without any obligation to give legal advice) if, in its opinion, to follow an instruction given by Customer would give rise to a breach of Applicable Privacy Law.

9. INTERNATIONAL DATA TRANSFERS

9.1 Customer agrees that Supplier may transfer Processed Personal Data to a country or territory outside the geographical area of Customer. If Supplier transfers Processed Personal Data to a country outside the applicable geographical area the transfer shall be made in full compliance with all Applicable Law.

The applicable geographical area includes Japan (Fujitsu Limited locates), Poland (Fujitsu Technology Solutions Sp. z o.o. locates), Netherlands, Ireland and the United Kingdom (Fujitsu Services and its server locates), India (Fujitsu Consulting India Private Limited locates), Australia (Fujitsu Australia Limited locates), the United States of America (server of Box service locates).

Europe Specific Provisions

9.2 Customer agrees that Supplier may transfer Processed Personal Data out of the European Economic Area and/or the United Kingdom (as applicable), to a country or territory outside that geographical area, subject always to the following conditions:

9.2.1 the transfer must be made in full compliance with all Applicable Law;

9.2.2 without limitation to clause 9.2.1 above, Supplier must:

9.2.2.1 provide appropriate safeguards in relation to the transfer;

9.2.2.2 ensure that the Data Subject has enforceable rights and effective legal remedies;

9.2.2.3 ensure there is an adequate level of protection for any Processed Personal Data transferred in accordance with Applicable Privacy Law; and

9.2.2.4 execute any additional contracts or documentation as is necessary to comply with Applicable Privacy Law.

9.3 The parties acknowledge that the transfer of Processed Personal Data from Customer to Supplier for the purpose of this Data Processing Addendum includes an international transfer of Processed Personal Data to a country outside the European Economic Area and/or the United Kingdom that is not considered adequate by the European Commission or the UK Secretary of State (as applicable) and as such the parties agree that Appendix 2: Standard Contractual Clauses shall apply to this Data Processing Addendum. Customer shall be the data exporter and Supplier shall be the data importer.

9.4 As of the date of this Data Processing Addendum, the parties have no reason to believe that the laws and practices in any third country of destination applicable to the Processed Personal Data, including any requirements to disclose Processed Personal Data or measures authorising access by a public authority, prevent the parties from complying with its obligations under this Data Processing Addendum.

10. DATA RETURN OR DESTRUCTION

On written request from Customer and in any event promptly following termination or expiry of the Agreement, Supplier shall delete or return to Customer all the Processed Personal Data in its possession or under its control, unless otherwise required by Applicable Law. In the case of return of the data, Supplier shall as soon as is practicable securely delete all other copies of the Processed Personal Data, unless otherwise required by Applicable Law.

11. MISCELLANEOUS

11.1 Governing Law and Jurisdiction: The construction, validity and performance of this Data Processing Addendum and all matters relating to the interpretation and effect of this Data Processing Addendum and non-contractual obligations arising from or connected with this Data Processing Addendum (and any amendment hereto) shall be governed by the laws as stated in the Agreement or if no governing law is stated in the Agreement the laws of England and Wales.

11.2 Invalidity: If any provision of this Data Processing Addendum (or part of any provision) is found by any court or other authority of competent jurisdiction to be invalid, illegal or unenforceable, that provision or part-provision shall, to the extent required, be deemed not to form part of this Data Processing Addendum,

and the validity and enforceability of the other provisions of this Data Processing Addendum shall not be affected.

APPENDIX 1: MINIMUM SECURITY REQUIREMENTS

Supplier maintains and enforces the technical and organisational measures as may be set out in the relevant Agreement or agreed in writing between the parties. The following is a description of some of the core technical and organizational security measures implemented by Supplier:

1.1 **Policies and Standards**

- Establish a policy framework of IT security, risk, and compliance management policies and guidelines. Integrate the controls based on appropriate risk assessments and evolving industry standards.
- Have an information security policy describing objectives, responsibilities and mandatory rules for protection of information. This policy should include data security controls such as data classification, physical security controls, encryption and training, among others. As an extension of such Information Security Policy, document the Process, procedures, organizational structures, and software and hardware functions.
- Maintain additional security standards, guidelines, and baselines which set forth further directions for implementation of specific, required controls such as internal firewalls and account and password management, among others.

1.2 **Information Classification and Access Control**

- Treat information required to conduct its business as a corporate asset, which must be protected against loss and infringements on integrity and confidentiality. Each organizational unit should be required by policy to assess risks to information assets and periodically check the level of security through security reviews.
- Information should be classified based on the nature of such information.
- All employees should be assigned unique User-IDs. Only authorized individuals should be able to grant, modify, or revoke access to an information system that uses or houses Personal Information, and access may be granted for valid business purposes only.
- User administration procedures should define user roles and their privileges, how access is granted, changed and terminated; address appropriate segregation of duties; and define the logging/monitoring requirements and mechanisms. Should maintain commercially reasonable physical and electronic security measures to create and protect passwords.

1.3 **System Integrity and Availability**

- Should maintain network security using commercially available equipment and commercially reasonable techniques.
- In the event of degradation or failure of the information infrastructure, should implement appropriate disaster recovery and business resumption plans. Back-up copies of critical business information and software should be created regularly and tested to ensure recovery.

- IT Security Controls should require appropriate logging and monitoring to enable recording of IT security related actions.

1.4 **Virus and Malware Controls**

- Should maintain anti-virus and malware protection software on its system.

1.5 **Security Incidents**

- All personnel should be required to report any observed or suspected Personal Information security incidents in accordance with appropriate incident reporting procedures.

1.6 **Physical Security**

- Should maintain commercially reasonable security systems at all sites at which an information system that uses or houses personal data is located. Secured areas should employ various physical security safeguards, including use of security badges (identity controlled access) and security guards stationed at entry and exit points. Visitors should only be provided access where authorized.

1.7 **Training & Compliance**

- Personnel should be required to read and abide by the IT security policies as a condition of employment.
- Should implement a security awareness program to train personnel about their security and privacy obligations. This program should include training about data privacy and security practices; physical security controls; and security incident reporting.
- Should regularly monitor the implemented security measures and implementation of new security requirements. Compliance with applicable policies and procedures should be accomplished through regular training, periodic reviews of local and organization-wide policies and procedures, and audits.

APPENDIX 2: STANDARD CONTRACTUAL CLAUSES

The rights and obligations afforded by the Standard Contractual Clauses will be exercised in accordance with this Data Processing Addendum, unless stated otherwise. In the event of any conflict or inconsistency between the Standard Contractual Clauses in this Appendix 2 and the body of the Data Processing Addendum, the Standard Contractual Clauses in this Appendix 2 shall prevail.

Controller to Processor

SECTION I

Clause 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 persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([i]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country 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 each 'data importer')

have agreed to these standard contractual clauses (hereinafter: '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.

Clause 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.

Clause 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), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

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

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined 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.

Clause 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.

Clause 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.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 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 importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described

in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. 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 importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([ii]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 14 day in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([iii]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 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.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

  (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

  (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 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) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) 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.

(f) The Parties agree that if one Party is held liable under paragraph (e), 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.

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

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the

representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 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 safeguard 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 ([iv]);

(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 data 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 exporter 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 request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, 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 reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter 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 exporter 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.

Clause 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 data 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 available 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 importer 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 importer 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 minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 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 importer 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 transfer 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.

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.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. 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 importer that prohibit the return or deletion of the transferred personal data, the data importer 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.

(e) 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.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Netherland (*specify Member State*).

[*This clause is deemed completed to include the governing law as stated in the Data Processing Addendum.]*

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Netherland (*specify Member State*).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

[A party's adherence to this Data Processing Addendum shall be deemed its signature of this Annex 1, all gaps below in this Annex 1 are deemed populated with the corresponding information from the Agreement and the Data Processing Addendum including Schedule 1: Data Processing Description.]

A. 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]*

Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller/processor):

2. …

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

Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller/processor):

2. …

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

...

Categories of personal data transferred

...

Sensitive 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 data, restrictions for onward transfers or additional security measures.

...

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

...

Nature of the processing

...

Purpose(s) of the 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

...

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

...

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 1

Netherland

ANNEX II

TECHNICAL AND ORGANISATIONAL ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

[This Annex II is populated with the corresponding information from Appendix 1: Security Requirements of the Data Processing Addendum].

ANNEX III

LIST OF SUB-PROCESSORS

[This Annex III is populated with the corresponding information from the relevant detail set out in the Data Processing Addendum.]