FUJITSU Cloud Service: Data Protection Addendum

June 22, 2018

This **Data Protection Addendum** (the "**Addendum**") forms part of the FUJITSU Cloud Service: TERMS OF USE (the "**Agreement**") between the Customer and Fujitsu.

In consideration of the mutual obligation set out in this Addendum, the parties agree that the terms and conditions set out below shall be added as an Addendum to the Agreement, to the extent that the GDPR applies to the Services described in this Addendum or elsewhere in the Agreement ("**Processing Services**"). Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum.

This Addendum applies only where Fujitsu processes personal data ("**Processed Personal Data**") as a processor on behalf of the Customer.

Terms not defined in this Addendum shall have the meaning given to them in the Agreement.

1. DATA PROCESSING

1.1 Defined terms

In this Addendum:

1.1.1 the terms "**controller**", "**data subject(s)**", "**personal data**", "**process**", "**processing**" and "**processor**" when used in this Addendum have the same meanings as in the GDPR (and their cognates are to be interpreted accordingly);

1.1.2 the following terms have the following meanings:

(a) "**Applicable Privacy Law**" means the GDPR or another applicable law or binding regulation on data protection or data privacy;

(b) "**GDPR**" means General Data Protection Regulation (EU) 2016/679;

(c) "**Services**" means the services provided or to be provided or procured by the Customer under the Agreement; and

(d) "**Sub-Processor**" has the meaning given in clause 1.5.1; and

1.1.3 the word "**including**" and its cognates are to be construed without limitation.

1.2 Processing Instructions

1.2.1 Fujitsu will only process the Processed Personal Data, and in particular only transfer any Processed Personal Data whose transfer is subject to the data privacy laws of the European Economic Area or the United Kingdom, respectively, to a country or territory outside that geographical area, including any transfer within a country or territory outside that geographical area, on the Customer's documented instructions.

1.2.2 The Customer hereby instructs Fujitsu to process the Processed Personal Data (including, without limitation, a transfer) as Fujitsu reasonably consider necessary to the performance of the Processing Services.

1.2.3 The Customer hereby irrevocably authorises Fujitsu to provide equivalent instructions to any Sub-Processors on its behalf.

1.3 Security Measures

Fujitsu will at all times have in place the technical and organisational security measures described in Schedule 1 to protect the Processed Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. The Customer confirms that it has reviewed those security measures, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing that Fujitsu will carry out on its behalf, and concluded that they are appropriate to the risks of varying likelihood and severity for the rights and freedoms of individuals that are presented by the processing.

1.4 Co-operation and Reasonable Assistance

1.4.1 Fujitsu will:

(a) take appropriate technical and organisational measures, insofar as is possible, to assist the Customer in responding to requests from data subjects for access to or rectification, erasure or portability of Processed Personal Data or for restriction of processing or objections to processing of Processed Personal Data (but Fujitsu will not itself respond to any such data subject request except on the Customer's written instructions); and

(b) give the Customer such assistance as it reasonably requests and Fujitsu is reasonably able to provide to ensure compliance with the Customer's security, data breach notification, impact assessment and data protection or data privacy authority consultation obligations under the applicable data privacy laws of the European Economic Area or the United Kingdom, taking into account the information available to Fujitsu.

1.4.2 Fujitsu may charge the Customer in accordance with the Agreement for time spent and expenses incurred in providing the Customer with co-operation and assistance as required by this clause 1.4.

1.5 Sub-Processors and Employees

1.5.1 The Customer hereby provides consent for Fujitsu to engage other processors ("**Sub-Processors**") to process the Processed Personal Data where Fujitsu is required to do so in order to provide the Processing Services. Where a Sub-Processor is appointed in accordance with this clause 1.5.1, the Customer hereby authorises Fujitsu to provide equivalent instructions of those set out in clause 1.2 to any Sub-Processors on its behalf. Fujitsu will ensure that any Sub-Processor is party to a written agreement binding on it with regard to the

Customer as controller and imposing obligations which are required under Article 28(3) of the GDPR.

1.5.2 Fujitsu will ensure that all of its employees authorised to have access to (or otherwise to process) the Processed Personal Data have committed themselves to confidentiality on appropriate terms or are under an appropriate statutory obligation of confidentiality.

1.6 **Audit**

1.6.1 Subject to clauses 1.6.2 and 1.6.3, and on reasonable advance written notice, Fujitsu will make available to the Customer such information as it reasonably requests and Fujitsu is reasonably able to provide, and, permit and contribute to such reasonable audits, including inspections, conducted by the Customer (or its appointed auditors), as reasonably necessary to demonstrate Fujitsu's compliance with this clause 1.

1.6.2 The Customer will make (and ensure that its auditors make) all reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to Fujitsu's premises, equipment, personnel and business while the Customer's or its auditors' personnel are on Fujitsu's premises in the course of such an audit or inspection. Fujitsu need not give access to its premises for the purposes of such an audit or inspection:

(a) to any individual unless he or she produces reasonable evidence of identity and authority;

(b) outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and the Customer has given prior written notice to Fujitsu that this is the case; or

(c) for the purposes of more than one audit or inspection in any calendar year, except for any additional audits or inspections which:

(i) the Customer reasonably considers necessary because of genuine concerns as to Fujitsu's compliance with this clause 1; or

(ii) the Customer is required or requested to carry out by applicable law or a competent data privacy authority,

where the Customer has identified its concerns or the relevant requirement or request in reasonable detail in its notice to Fujitsu of the audit or inspection.

1.6.3 Clause 1.6.1 does not require Fujitsu to disclose to the Customer or its auditors any information disclosed to Fujitsu in confidence by, or otherwise held by Fujitsu in confidence on behalf of, any of its other customers or any other person.

1.7 **Deletion or Return of Processed Personal Data**

1.7.1 Subject to clause 1.7.2, when provision of the Processing Services is complete, or earlier if the Customer withdraws its instructions, Fujitsu will as soon as is practicable delete (or return to the Customer, at its option - to be exercised by written notice before the earlier of completion of provision of the Processing Services and withdrawal of its instructions) any Processed Personal Data in Fujitsu's possession or under its control which is subject to the data privacy laws of the European Economic Area or the United Kingdom.

1.7.2 However, clause 1.7.1 does not require Fujitsu to delete or return Processed Personal Data which it is required to retain by the law or regulation of a member state of the European Economic Area or the United Kingdom (as the case may be) or any copies of Processed Personal Data which it is not technically practicable for Fujitsu to locate and delete or return.

1.8 **International Data Transfers**

1.8.1 The Customer (for itself and as agent for its affiliates) (as data exporter) and Fujitsu (as data importer) hereby enter into a data transfer agreement in the form set out in Schedule 2 (*Form of Data Transfer Agreement*) in relation to transfers of Processed Personal Data from the Customer to Fujitsu.

1.8.2 The Customer acknowledges that Fujitsu may use Sub-Processors, including its own affiliates, outside the EEA to process the Processed Personal Data.

1.8.3 Before Fujitsu or any of its Sub-Processors transfers (or requires the Customer in the receipt of the Services to transfer) any Processed Personal Data subject to the GDPR or any Applicable Privacy Laws of the EEA to a Sub-Processor in a country or territory outside that geographical area, Fujitsu shall ensure that:

(a) that country or territory has been decided to ensure adequate protection for personal data (or categories of personal data which include those Processed Personal Data) in accordance with the GDPR; or

(b) Fujitsu, as agent for the Customer, has entered into a data transfer agreement with the Sub-Processor in an appropriate form approved by the relevant competent body under the GDPR as providing appropriate safeguards to protect personal data and populated so that it applies to the transfer.

1.8.4 The Customer hereby irrevocably authorises Fujitsu to enter into data transfer agreements as referred to in clause 1.8.3(b) as agent on behalf of the Customer, including by ratification of Fujitsu having entered into such agreements before the date of the Agreement.

2. **GOVERNING LAW AND JURISDICTION**

2.1 The parties submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum, including

disputes regarding its existence, validity or termination or the consequences of its nullity.

2.2 This Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for the equivalent purpose in the Agreement.

3. ORDER OF PRECEDENCE

3.1 Except as modified by this Addendum, the terms of the Agreement shall remain in full force and effect.

3.2 Nothing in this Addendum reduces Customer's or any other of its affiliates' obligations under the Agreement in relation to the protection of personal data or permits Customer or any of its affiliates to process (or permit the processing of) personal data in a manner which is prohibited by the Agreement.

3.3 Subject to clause 3.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Agreement, the provisions of this Addendum shall prevail.

4. SEVERANCE

Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

SCHEDULE 1
SECURITY MEASURES

Information Classification and Access Control

Fujitsu regards 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 assess risks by policy to information assets and periodically check the level of security through security reviews.

Information is classified based on the nature of such information, such as Tier One Information, Fujitsu Information, Third-Party Information, Internal Use Only Information, and Public Information, and each classification controls appropriate levels of security (e.g., encryption of data classified as restricted or confidential).

All employees of Fujitsu are assigned unique User-IDs. Only authorized individuals grant, modify, or revoke access to an information system that uses or houses personal data, and access may be granted for valid business purposes only.

User administration procedures 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. Fujitsu maintains commercially reasonable physical and electronic security measures to create and protect passwords.

System Integrity and Availability

Fujitsu maintains network security using commercially available equipment and industry standard techniques, including firewalls, intrusion detection and/or prevention systems, access control lists and routing protocols.

In the event of degradation or failure of the information infrastructure, Fujitsu implements appropriate disaster recovery and business resumption plans. Back-up copies of critical business information and software are created regularly and tested to ensure recovery. Fujitsu reviews and assesses periodically the Business Continuity Plan.

IT Security Controls are appropriately logging and monitoring to enable recording of IT security related actions.

Virus and Malware Controls

Fujitsu maintains anti-virus and malware protection software on its system.

Security Incidents

All personnel of Fujitsu report any observed or suspected Personal Information security incidents in accordance with appropriate incident reporting procedures.

Physical Security

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

SCHEDULE 2
FORM OF DATA TRANSFER AGREEMENT

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, the Customer and Fujitsu have agreed on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data'*, *'special categories of data'*, *'process/processing'*, *'controller'*, *'processor'*, *'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which

case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

Data exporter

The data exporter is: Customer

Data importer

The data importer is: Fujitsu Limited

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Customer Employees

Categories of data

The personal data transferred concern the following categories of data:

- Personal details within contract and invoice data, containing data related to Customer employees;
- Communication data between Customer and Fujitsu.
- Corporate profile information, email and support ticket logs related to support correspondence between the Customer's contact people and Fujitsu (including the email address and IP address of the Customer's email client application),
- Intrusion Detection System logs (including source IP address and destination IP address,
- Other machine logs associated with the operation of Processing Services and their supporting systems,
- Any personal data contained within the Customer Business Data, in case Customer transferred Business Data to the Cloud Service environment outside the EEA at its sole discretion.

"**Customer Business Data**" means data placed on or produced within the Cloud Service environment by Customers through the normal operation of their hosted business services, or for their own business purposes.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

N/A

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Collection, recording, use, disclosure by transmission, or otherwise making available to the extent necessary for the provision of Processing Services.

Appendix 2 to the Standard Contractual Clauses

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

The technical and organizational measures set forth in Schedule 1 of FUJITSU Cloud Service: Data Protection Addendum are hereby incorporated into this Appendix 2 by this reference and are binding on the data importer as if they were set forth in this Appendix 2 in their entirety.

Supplementary Provision (May 24, 2018)

The present Data Protection Addendum is effective from May 24, 2018.

Supplementary Provision (June 22, 2018)

The present Data Protection Addendum is effective from June 22, 2018.