Fujitsu Computing as a Service: Data Protection Addendum

June 1st, 2023

This **Data Protection Addendum** (the "**Addendum**") forms part of the Fujitsu Computing as a 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 for the transfer of personal data from the Community to third countries: Controller to Processor - Module Two

Name of the data exporting organisation:

Address:

hereinafter "**Customer**"

and

Name of the data importing organisation**: Fujitsu Limited**

Address**:**

hereinafter "**data importer**"

each a "party"; together "the parties".

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) for the transfer of personal 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
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 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 (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) SPECIFIC PRIOR AUTHORISATION: The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 30 days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(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. 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.

Clause13
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

Clause14
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;

(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.

Clause15

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

Clause16
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.

Clause17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause18

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 Germany.

(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. LIST OF PARTIES

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

1. Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date: Effective date of the Agreement

Role: Controller

2.

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

1. Name: Fujitsu Limited

Address: Shiodome City Center, 1-5-2 Higashi-Shimbashi, Minato-ku, Tokyo Japan

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

Supportdesk Contactline

contact-caas-helpdesk@cs.jp.fujitsu.com

Activities relevant to the data transferred under these Clauses: Communication, Hosting Data, Analysing system or any other machine logs

Signature and date: Effective date of the Agreement

Role: Processor

B. DESCRIPTION OF TRANSFER

1. Categories of data subjects whose personal data is transferred ((multiple selections possible)

Service customer (Natural Person), including

- Signer who signed up Fujitsu Computing as a Service as a customer.

- Manager assigned by the signer.

- Engineer assigned by the signer.

2. Categories of personal data transferred (multiple selections possible)

- Natural person's e-mail address, login ID/password associated with the e-mail address, and his/her contact information.

3. Sensitive data transferred (if applicable) (multiple selections possible)

N/A

4. The frequency of the transfer

Anytime

5. Nature of the processing (multiple selections possible)

- Add/Modify/Remove personal information, as a personal data, into/from Fujitsu Computing as a Service account management system.

6. Purpose(s) of the data transfer and further processing

- Verify and authenticate ID and password entered by the customer, to authorize access to Fujitsu Computing as a Service.
- Use e-mail address and/or contact information to contact customer (service update - announcement, technical support, QA, etc.)

7. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

- Until customer cancels use of Fujitsu Computing as a Service, or
- The signer/manager/engineer removes his/her ID and contact information, or
- Fujitsu permanently terminated Fujitsu Computing as a Service.

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

- Fujitsu Limited

- Sub-processer (described in Annex Ⅲ)

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

• 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 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 shall act as the 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: Dutch Data Protection Authority shall act as the competent supervisory authority.

• Where the data exporter is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws and Regulations, the Information Commissioner's Office shall act as the competent supervisory authority.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The data importer shall implement such technical and organisational security measures for Processing of any Personal Data as provided in the Agreement and shall upon written request from provide evidence of the implementation of such measures.

The data importer must have in place and maintain at least the following technical and organisational security measures:

Equipment Access Control: The Data importer shall take reasonable technical and organisational measures to deny unauthorised persons access to processing equipment used for processing. Unauthorised persons shall be prevented from gaining physical access to premises, buildings or rooms, where data processing systems are located which process Personal Data; persons are unauthorised if their activity does not correspond to tasks assigned to them. Exceptions may be granted for the purpose of auditing the facilities to third party auditors as long as they are supervised by the Data importer and do not get access to the Processed Personal Data itself.

The Data importer shall in particular:

Specify authorized individuals

Use an access control process to avoid unauthorized access to office rooms

Have a access control process to restrict access to data center/rooms were servers are located

Use video surveillance and alarm devices with reference to access areas

Personnel without access authorization (e.g. technicians, cleaning personnel) has to be accompanied all times

[Complete and describe your technical and organizational measures you have implemented in detail or confirm the listed activities above.]

- Specify authorized individuals
- Use an access control process to avoid unauthorized access to office rooms
- Have an access control process to restrict access to data center/rooms where servers are located
- Use video surveillance and alarm devices with reference to access areas
- Personnel without access authorization (e.g. technicians, cleaning personnel) has to be accompanied all times

☐ We confirm the measures as listed above (2.1. a-e)

Data Media Control: The Data importer shall take reasonable technical and organisational to prevent the unauthorised reading, copying, modification or removal of data media.

The Data importer shall in particular:

store data media in secured areas

establish rules for the safe and permanent destruction of data media that are no longer required

only grant Data importer personnel and its Sub-Contractors' directors, officers, employees, agents, permitted subcontractors and assigns minimal permissions to access data media as needed to fulfil their function

[Complete and describe your technical and organizational measures you have implemented in detail or confirm the listed activities above.]

- Prohibit use and/or transfer of removal data media.
- Establish rules for the safe and permanent destruction of data media, that are no longer required, which is installed into the data centre with secure and restricted access.
- Only grant Data importer personnel and its Sub-Contractors' directors, officers, employees, agents, permitted subcontractors and assigns minimal permissions to access data media as needed to fulfil their function

☐ We confirm the measures as listed above (2.2. a-c)

Storage Control: The Data importer shall take reasonable technical and organisational to prevent the unauthorised input of Processed Personal Data and the unauthorised inspection, modification or deletion of Processed Personal Data. Persons entitled to use a data processing system shall be able to input and gain access only to the data to which they have a right of input or access, and Processed Personal Data must not be read, copied, modified or removed without authorization in the course of processing

The Data importer shall in particular:

restrict access to files and programs based on a "need-to-know-basis"

store data carriers in secured areas

prevent use/installation of unauthorized hardware and/or software

establish rules for the safe and permanent destruction of data that are no longer required

only grant Data importer personnel and its Sub-Contractors' directors, officers, employees, agents, permitted subcontractors and assigns minimal permissions to access data as needed to fulfil their function

[Complete and describe your technical and organizational measures you have implemented in detail or confirm the listed activities above.]

- Restrict access to files and programs based on a "need-to-know-basis"
- Prevent use/installation of unauthorized hardware and/or software
- Establish rules for the safe and permanent destruction of data that are no longer required
- Only grant Data importer personnel and its Sub-Contractors' directors, officers, employees, agents, permitted subcontractors and assigns minimal permissions to access data as needed to fulfil their function

☐ We confirm the measures as listed above (2.3. a-e)

User Control: The Data importer shall take reasonable technical and organisational to prevent the use of automated processing systems by unauthorised persons using data communication equipment.

The Data importer shall in particular:

take reasonable measures to protect systems processing Processed Personal Data against unauthorised access by means of data communication equipment, including the deployment of firewalls and intrusion detection systems;

log remote access to systems processing Processed Personal Data;

ensure that the remote access control is supported by an authentication system

only grant Data importer personnel, or its Sub-Contractors' directors, officers, employees, agents, and assigns remote access to applications which process Processed Personal Data to the extent they require to fulfil their function

have a proper procedure to deactivate remote access accounts, when user leaves company or function

[Complete and describe your technical and organizational measures you have implemented in detail or confirm the listed activities above.]

- Take reasonable measures to protect systems processing Processed Personal Data against unauthorised access by means of data communication equipment, including the deployment of firewalls and intrusion detection systems.
- Log remote access to systems processing Processed Personal Data.
- Ensure that the remote access control is supported by an authentication system
- Only grant Data importer personnel, or its Sub-Contractors' directors, officers, employees, agents, and assigns remote access to applications which process Processed Personal Data to the extent they require to fulfil their function
- Have a proper procedure to deactivate remote access accounts when user leaves company or function.

☐ We confirm the measures as listed above (2.4. a-e)

Data Access Control: The Data importer shall take reasonable technical and organisational to ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation. Data processing systems must be prevented from being used without authorization.

The Data importer shall in particular:

ensure that all computer processing Processed Personal Data (incl. remote) are password protected

- after boot sequences
- when left even for a short period

to prevent someone else from unauthorised access to Processed Personal Data

have dedicated user IDs for authentication against systems user management for every individual

assign individual user passwords for authentication

ensure that the access control is supported by an authentication system, including access and use of systems by way of remote access

only grant Data importer personnel, or its Sub-Contractors' directors, officers, employees, agents, and assigns access to applications which process Processed Personal Data to the extent they require to fulfil their function

Implement a password policy that prohibits the sharing of passwords, outlines processes after a disclosure of a password and requires the regular change of passwords

ensure that each computer has a password protected screensaver, that is activated at least after 10-15 minutes of inactivity

ensure that passwords are always stored in encrypted form

have a proper procedure to deactivate user account, when user leaves company or function

have a proper process to adjust administrator permissions, when an administrator leaves company/function

[Complete and describe your technical and organizational measures you have implemented in detail or confirm the listed activities above.]

- All computer processing Processed Personal Data (incl. remote) are password protected
  - after boot sequences
  - when left even for a short period

  to prevent someone else from unauthorised access to Processed Personal Data

- Have dedicated user IDs for authentication against systems user management for every individual
- Assign individual user passwords for authentication
- Access control is supported by an authentication system, including access and use of systems by way of remote access
- Only grant Data importer personnel, or its Sub-Contractors' directors, officers, employees, agents, and assigns access to applications which process Processed Personal Data to the extent they require to fulfil their function
- Implement a password policy that prohibits the sharing of passwords, outlines processes after a disclosure of a password and requires the regular change of passwords
- Ensure that each computer has a password protected screensaver, that is activated at least after 5 minutes of inactivity
- Passwords are always stored in encrypted form
- Have a proper procedure to deactivate user account, when user leaves company or function
- Have a proper process to adjust administrator permissions when an administrator leaves company/function

☐ We confirm the measures as listed above (2.5. a-j)

Communication Control: The Data importer shall maintain adequate records and documentation to verify and establish the bodies to which Processed Personal Data have been or may be transmitted or made available by the Data importer or any of its Sub-Contractors using data communication equipment.

[Complete and describe your technical and organizational measures you have implemented in detail.]

Customer services records such as technical support or inquiry have been recorded in the service tickets.

Input Control: The Data importer shall take reasonable technical and organisational to ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input. It shall be possible retrospectively to examine and establish whether and by whom Processed Personal Data have been entered into data processing systems, modified or removed (to the extent this is under the Data importer's control).The Data importer shall in particular, in its and its Sub-Contractor's organisation:

log administrators and user activities

permit only authorized personnel to enter and modify any Processed Personal Data within the scope of their function

[Complete and describe your technical and organizational measures you have implemented in detail or confirm the listed activities above.]

- Log administrators and user activities
- Permit only authorized personnel to enter and modify any Processed Personal Data within the scope of their function

☐ We confirm the measures as listed above (2.7. a-b)

Transport Control: The Data importer shall take reasonable technical and organisational to prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media. Except as necessary for the provision of the Services in accordance with the Main Agreement, Processed Personal Data must not be read, copied, modified or removed without authorization during transfer or storage and it shall be possible to establish to whom Processed Personal Data was transferred to and the Data importer shall take reasonable measures to protect the confidentiality and integrity of Processed Personal Data during transfer and transport.

The Data importer shall in particular:

encrypt data during any transmission using strong and state-of-the-art encryption algorithms (please describe)

transport data carriers in sealed containers

have shipping and delivery notes

[Complete and describe your technical and organizational measures you have implemented in detail or confirm the listed activities above.]

N/A (or Data importer and its sub-contractor will never transfer personal data to/from data media.)

☐ We confirm the measures as listed above (2.8. a-c)

Recovery: The Data importer shall take reasonable technical and organisational to ensure that installed systems may, in the case of interruption, be restored.

The Data importer shall in particular:

create back-up copies stored in specially protected environments (to the extent this is part of the Services)

perform regular restore tests from those backups

create contingency plans or business recovery strategies for its own operations

not remove Processed Personal Data from the Data importer's business computers or premises for any reason (unless the data exporter has specifically authorized such removal for business purposes).

not use private equipment to perform the Services

run an up to date antivirus solution on computer systems

[Complete and describe your technical and organizational measures you have implemented in detail or confirm the listed activities above.]

- Create back-up copies stored in specially protected environments
- Create contingency plans or business recovery strategies for its own operations
- Not remove Processed Personal Data from the Data importer's business computers or premises for any reason (unless the data exporter has signed off the service and/or specifically authorized such removal for business purposes).
- Not use private equipment to perform the Services
- Run an up to date antivirus solution on computer systems

☐ We confirm the measures as listed above (2.9. a-f)

Reliability: The Data importer shall take reasonable technical and organisational to ensure that the functions of the system perform, that the appearance of faults in the functions is reported. Reference is made to the specification of the Service, including service levels and quality requirements, and the reporting obligations of the Data importer as specified in the Main Agreement.

Integrity: The Data importer shall take reasonable technical and organisational to ensure that stored Processed Personal Data cannot be corrupted by means of a malfunctioning of the system. Reference is made to the specification of the Service, including service levels and quality requirements, and the reporting obligations of the Data importer as specified in the Main Agreement.

[Complete and describe your technical and organizational measures you have implemented in detail.]

- The system where the personal data is stored have been implemented with resilient and fault-tolerant capability.

Contractual Control: Processed Personal Data being processed on commission shall be processed solely in accordance with the Main Agreement and related instructions. The Data importer will carry out the Services and, in particular, the data processing services for Processed Personal Data only in accordance with given instructions, and will instruct its personnel and Sub-Contractors involved in the processing of Processed Personal Data accordingly:

The Data importer shall in particular:

establish controls of the contractual performance

work according to written instructions or contracts

process the Processed Personal Data received from different clients to ensure that in each step of the processing the data controller of the Processed Personal Data can be identified (physical or logical separation of data)

[Complete and describe your technical and organizational measures you have implemented in detail or confirm the listed activities above.]

- Establish controls of the contractual performance
- Work according to written instructions or contracts
- Process the Processed Personal Data received from different clients to ensure that in each step of the processing the data controller of the Processed Personal Data can be identified (physical or logical separation of data)

☐ We confirm the measures as listed above (2.12. a-c)

Availability Control: Processed Personal Data shall be protected against disclosure, accidental or unauthorized destruction or loss.

The Data importer shall in particular:

create back-up copies stored in specially protected environments (to the extent this is part of the Services)

create contingency plans or business recovery strategies for its own operations

not use Processed Personal Data for any purpose other than what have been contracted to perform

not remove Processed Personal Data from the Data importer's business computers or premises for any reason (unless the date exporter has specifically authorized such removal for business purposes).

not use private equipment to perform the Services

whenever a user leaves his desk unattended during the day, and prior to leaving the office at the end of the day, he/she must ensure that documents containing Processed Personal Data are placed in a safe and secure environment such as a locked desk drawer, filing cabinet, or other secured storage space (clean desk)

implement a process for disposal of documents or data carriers containing personal data

have firewalls on network level to prevent unauthorized access to systems and services on network level

run an up to date antivirus solution on computer systems

[Complete and describe your technical and organizational measures you have implemented in detail or confirm the listed activities above.]

- Create back-up copies stored in specially protected environments (to the extent this is part of the Services)
- Create contingency plans or business recovery strategies for its own operations
- Not use Processed Personal Data for any purpose other than what have been contracted to perform
- Not remove Processed Personal Data from the Data importer's business computers or premises for any reason (unless the date exporter has specifically authorized such removal for business purposes).
- Not use private equipment to perform the Services
- Whenever a user leaves his desk unattended during the day, and prior to leaving the office at the end of the day, he/she must ensure that documents containing Processed Personal Data are placed in a safe and secure environment such as a locked desk drawer, filing cabinet, or other secured storage space (clean desk)
- Implement a process for disposal of documents or data carriers containing personal data
- Have firewalls on network level to prevent unauthorized access to systems and services on network level
- Run an up to date antivirus solution on computer systems

☐ We confirm the measures as listed above (2.13. a-j)

Separation: The Data importer shall take such technical and organisational measures as set forth in the Main Agreement to ensure that Processed Personal Data collected for different purposes can be processed separately. The Data importer shall be entitled to rely on the instructions of and information provided by the Customer in this respect, in particular in relation the types of Processed Personal Data and the purpose of collection.

To the extent that any measures required to separate data are not within the Data importer's obligations under the Main Agreement, the Data importer's obligation to implement such measures remain subject to agreement on (i) the specification of such measures and (ii) a reasonable remuneration of the Data importer.

[Complete and describe your technical and organizational measures you have implemented in detail.]

- Personal Data is collected and used for the purpose of authenticate and grant access to data exporter's business data by log into Fujitsu Computing as a Service portal using the ID associate with the personal data. The data exporter can only access to their business data.
- Personal Data (contact information) is used for the purpose of service update notification and/or technical support /QA communication purpose.

2.15 **Organisational Requirements**: The internal organisation of the Data importer shall meet the specific requirements of data protection. In particular, to avoid accidental mixing of Processed Personal Data, the Data importer separates other data than that belonging to Data Exporter by technical and organisational measures from Data Importer data.

The Data importer shall in particular:

(a) designate a Data Protection Officers

(b) get the commitment of the employees to maintain confidentiality

(c) train staff on data privacy and data security

(d) have in place processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of processing

(e) have in place measures for certification/assurance of processes and products

(f) ensure that an internal IT and IT security governance and management is established (e.g. ISO 27001:2013 or later)

[Complete and describe your technical and organizational measures you have implemented in detail or confirm the listed activities above.]

The Data importer:

(a) assigns a designate a Data Protection Officers
(b) gets the commitment of the employees to maintain confidentiality
(c) trains staff on data privacy and data security

(d) has in place processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of processing
(e) has in place measures for certification/assurance of processes and products
(f) ensure that an internal IT and IT security governance and management is established

☐ We confirm the measures as listed above (2.15. a-f)

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Name:

Address:

Address:

URL:

Supplementary Provision (October 25th, 2022)

The present Data Protection Addendum is effective from October 25th, 2022.

Supplementary Provision (June 1st, 2023)

The present Data Protection Addendum is effective from June 1st, 2023.