Docmosis – Data Processing Addendum

This Data Processing Addendum ("**Addendum**") to the Cloud Services Agreement, located at https://www.docmosis.com/CSA (the "**Agreement**"), between: the Customer identified in the signature block below ("**Customer**") and Docmosis Pty Ltd **(**"**Docmosis**"**)** is dated the later of (i) 25th of May, 2018 or (ii) the date of last signature of a party below **(**"**Effective Date**"**)**

The capitalized terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and related terms shall be construed accordingly:

1.1.1 "**Applicable Laws**" means (a) EU Data Protection Laws or Member State laws which apply to any Customer Personal Data; and (b) any other applicable law which applies to any Customer Personal Data;

1.1.2 "**Customer Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of the Customer pursuant to or in connection with the Agreement;

1.1.3 "**Contracted Processor**" means Docmosis or a Subprocessor;

1.1.4 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

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

1.1.6 "**EU Data Protection Laws**" means the GDPR, and any domestic legislation of each Member State implementing the GDPR, as amended, replaced or superseded from time to time;

1.1.7 "**GDPR**" means 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;

1.1.8 "**Services**" means the Cloud Services and other activities to be supplied to or carried out by or on behalf of Docmosis to the Customer pursuant to the Agreement;

1.1.9 "**Standard Contractual Clauses**" means the contractual clauses set out in Schedule 4;

1.1.10 "**Subprocessor**" means any person (including any third party, but excluding an employee of Docmosis or any of its sub-contractors) appointed by or on behalf of Docmosis to Process Personal Data on behalf of the Customer in connection with the Agreement; and

1.1.11 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their related terms shall be construed accordingly.

1.2 The word "**include**" shall be construed to mean include without limitation, and related terms shall be construed accordingly.

2. Processing of Customer Personal Data

2.1 Docmosis shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Customer Personal Data; and

2.1.2 not Process Customer Personal Data other than on the Customer's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Docmosis shall to the extent permitted by Applicable Laws inform the Customer of that legal requirement before the relevant Processing of that Personal Data.

2.2 As part of the agreed delivery of the Services, Docmosis will process Customer Personal Data for and on behalf of, and solely in accordance with the documented instructions of Customer and any Applicable Laws. Additional written instructions may be issued and amended by Customer from time to time.

2.3 The Customer instructs Docmosis (and authorises Docmosis to instruct each Subprocessor) only to Process Customer Personal Data as reasonably necessary for the provision of the Services and consistent with the Agreement.

2.4 The Customer agrees that this Addendum is Customer's, as of the Effective Date, complete and final instructions to Docmosis in relation to processing Customer Personal Data.

2.5 Schedule 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of Customer Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Processing outside the scope of this Addendum (if any) will require prior written agreement between Docmosis and Customer on additional instructions for processing, including agreement on any additional fees Customer will pay to Docmosis for carrying out such instructions. Customer may terminate this Addendum if Docmosis declines to follow instructions requested by Customer that are outside the scope of this Addendum. Nothing in Schedule 1 (including as amended pursuant to this section 2.5) confers any right or imposes any obligation on any party to this Addendum.

2.6 The parties agree that Schedule 4 (Standard Contractual Clauses) applies in relation to Docmosis Processing of Customer Personal Data in addition to what is set out in this Addendum. In the event of any inconsistencies between the two sets of terms, the provisions that establish the most comprehensive obligations on the processor shall hold precedence.

3. Docmosis Personnel

Docmosis shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Customer Personal Data, as strictly necessary

for the purposes of the Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Docmosis shall in relation to Customer Personal Data implement and maintain appropriate security measures to ensure a level of security appropriate to that risk in accordance with Article 32 of the GDPR, and include the measures described in Schedule 2.

4.2 Customer acknowledges that any security measures are subject to technical progress and development and that Docmosis may update or modify the security measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services provided to the Customer.

4.3 Notwithstanding the above, Customer agrees that except as provided by this Addendum, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Personal Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Personal Data uploaded to the Services.

5. Subprocessing

5.1 The Subprocessors currently engaged by Docmosis and authorized by Customer are listed in Schedule 3. The Customer generally authorises Docmosis to appoint (and permit each Subprocessor appointed in accordance with this section 5 to appoint) Subprocessors in accordance with this section 5 and any restrictions in the Agreement.

5.2 Docmosis may continue to use those Subprocessors already engaged by Docmosis as at the date of this Addendum, subject to Docmosis in each case as soon as practicable meeting the obligations set out in section 5.4.

5.3 Docmosis shall give Customer prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within 30 days of receipt of that notice, Customer notifies Docmosis in writing of any objections (on reasonable grounds) to the proposed appointment Customer may by written notice to Docmosis with immediate effect terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Subprocessor. This termination right is Customer’s sole and exclusive remedy if Customer objects to any new Third Party Subprocessor. Under no circumstances shall a Subprocessor be given access to Customer Personal Data or provide any of the Services before the above mentioned 30 days period has expired or if the Customer has issued an objection to the relevant Subcontractor pursuant to this section 5.

5.4 With respect to each Subprocessor, Docmosis shall:

5.4.1 before the Subprocessor first Processes Customer Personal Data (or, where relevant, in accordance with section 5.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Customer Personal Data required by the Agreement;

5.4.2 ensure that the arrangement between on the one hand (a) Docmosis, or (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Customer Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;

5.4.3 provide to Customer for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Customer may request from time to time.

5.5 Docmosis shall ensure that each Subprocessor performs the obligations under sections 2.1, 3, 4, 7.1, 8.2, 9 and 11.1, as they apply to Processing of Customer Personal Data carried out by that Subprocessor, as if it were party to this Addendum in place of Docmosis.

6. Data Location and Transfers outside the EU/EEA

6.1 Docmosis shall not transfer or make accessible any Customer Personal Data to any jurisdiction or international organisation outside the EU/EEA area (a "**Transfer**"), unless: i) Docmosis obtains Customer's prior written approval, and ii) the actions of Docmosis is permitted under Applicable Law.

6.2 The approval of Customer shall be conditional on Docmosis taking all such steps (and procuring that Docmosis' personnel take all such steps) that Customer may deem necessary to ensure an adequate level of protection for the personal data in accordance with Customer's instructions and the Data Protection Laws. Such measures may include (without limitation), and in Customer's sole discretion, Docmosis and its sub-processors entering into standard contractual clauses adopted by the European Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679 ("SCCs"), and the provisioning of Transfer Impact Assessments. In case Customer approves the transfer of customer or Customer Personal Data to a country outside the EU/EEA, the Processor shall ensure that the Transfer complies with Chapter V of the GDPR, and applicable bank secrecy and data privacy regulations must be adhered to.

6.3 The location of personal data or Customer Personal Data shall be specified in Schedule 3.

6.4 Any change or modification in the location of personal data or Customer Personal Data is subject to Customer's prior written approval.

7. Data Subject Rights

7.1 Taking into account the nature of the Processing, Docmosis shall assist the Customer by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.2 Docmosis shall:

7.2.1 promptly notify Customer if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and

7.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Customer or as required by Applicable Laws to which the Contracted Processor is subject, in which case Docmosis shall to the extent permitted by Applicable Laws inform Customer of that legal requirement before the Contracted Processor responds to the request.

8. Personal Data Breach

8.1 Docmosis shall notify Customer without undue delay upon Docmosis or any Subprocessor becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer, to the extent possible, with sufficient information to allow the Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

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

8.3 Docmosis's notification of or response to a Personal Data Breach under this section 8 will not be construed as an acknowledgement by Docmosis of any fault or liability with respect to the Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

Docmosis shall provide commercially reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

10. Deletion or return of Customer Personal Data

10.1 Customer acknowledges and agrees that Customer will be responsible for exporting, before the date of cessation of any Services involving the Processing of Customer Personal Data (the "**Cessation Date**"), any Customer Personal Data it wishes to retain.

10.2 Subject to section 10.3 Docmosis shall as soon as reasonably practical and in any event within 90 days of the the Cessation Date, delete and procure the deletion of all copies of those Customer Personal Data.

10.3 Each Contracted Processor may retain Customer Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Docmosis shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

11. Audit rights

11.1 If the GDPR applies to the processing of Customer Personal Data, and subject to sections 11.2 to 11.7, Docmosis shall make available to the Customer on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by Customer or an auditor mandated by Customer in relation to the Processing of Customer Personal Data by the Contracted Processors.

11.2 Information and audit rights of the Customer only arise under section 11.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

11.3 Following receipt by Docmosis of a request under section 11.1, Docmosis and Customer will discuss and agree in advance on the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit under section 11.1.

11.4 Docmosis may charge a fee (based on Docmosis's reasonable costs) for any audit under section 11.1, however always subject to Customer's prior written approval. Docmosis will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to conduct any such audit, however always subject to Customer's prior written approval.

11.5 Docmosis may object in writing to an auditor appointed by Customer to conduct any audit under section 11.1 if the auditor is, in Docmosis's reasonable opinion, not suitably qualified or independent, a competitor of Docmosis or otherwise manifestly unsuitable. Any such objection by Docmosis will require Customer to appoint another auditor or conduct the audit itself.

11.6 Customer undertaking an audit under section 11.1 shall make (and ensure that each of its mandated auditors makes) reasonable endeavors to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection.

11.7 A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

11.7.1 to any individual unless he or she produces reasonable evidence of identity and authority;

11.7.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Customer undertaking an audit has given notice to Docmosis that this is the case before attendance outside those hours begins; or

11.7.3 for the purposes of more than one audit or inspection, in respect of each Contracted Processor, in any calendar year, except for any additional audits or inspections which:

11.7.3.1 Customer undertaking an audit reasonably considers necessary because of genuine concerns as to Docmosis's compliance with this Addendum; or

11.7.3.2 Customer is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

where Customer undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Docmosis of the audit or inspection.

12. General Terms

Governing law and jurisdiction

12.1 The parties to this Addendum hereby 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; and 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 this purpose in the Agreement.

Order of precedence

12.2 Nothing in this Addendum reduces Docmosis's obligations under the Agreement in relation to the protection of Personal Data or permits Docmosis to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Agreement.

12.3 Subject to section 12.2, 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 and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Severance

12.4 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.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Agreement with effect from the Effective Date.

On behalf of Customer:

Signature : _____

Signer's Name : _____

Position : _____

Date Signed : .....

On behalf of Docmosis:

Signature : _____

Signer's Name : _____

Position : _____

Date Signed : .....

Schedule 1

Details of Processing

Data Controller:

Name : _____

Address : _____

_____

_____

Data Processor:

Name : **Docmosis Pty Ltd**

Address : Suite 8 / 5 Hasler Rd

Osborne Park, WA 6017,

Australia

This Schedule includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR.

Subject matter of the Processing of Customer Personal Data

The subject matter of the Processing of the Customer Personal Data is the provision of the Cloud Services as set out in the Agreement and this Addendum.

Docmosis has no control or visibility as to whether any data sent to be Processed by the Services is in fact Customer Personal Data.

Duration of the Processing of Customer Personal Data

Customer Personal Data will be processed by Docmosis for the Customer for the duration of the Agreement.

The nature and purpose of the Processing of Customer Personal Data

Customer, as a client of Docmosis, may use the Services to perform processing activities that include: access, structuring, adaptation, formatting, and erasure for the purpose of automated document generation in performance of the Agreement.

The types of Customer Personal Data to be Processed

The type of Customer Personal Data that Customer may submit to the Services to be Processed, the extent of which is determined and controlled by Customer in its sole discretion, may include, but is not limited to, Customer's clients' Personal Data and other Personal Data concerning Customer's employees, contractors, collaborators, customers, prospects, suppliers and subcontractors.

Docmosis no control or visibility as to the type of Customer Personal Data sent to be Processed by the Services.

The categories of Data Subject to whom the Customer Personal Data relates

Customer has complete control over the categories of Data Subject it sends to be Processed by the Services.

Docmosis no control or visibility as to the categories of Data Subject sent to be Processed by the Services.

The obligations and rights of Customer

The obligations and rights of Customer are set out in the Agreement and this Addendum.

Customer must follow the “Guidelines for Using the Docmosis Cloud Services in a GDPR-Compliant Manner” issued by Docmosis (dated 02 Aug 2023).

Schedule 2

Technical and Organizational Measures

Docmosis will implement and maintain the measures set out below.

1. Physical Security

1.1. Processing shall occur entirely on Amazon Web Services (AWS) infrastructure, providing comprehensive physical security as well as the logical facilities supporting the non-physical system security.

1.2. Docmosis premises shall have physical access control systems and be protected after hours by an externally monitored security system.

2. Logical Security

Docmosis shall implement systems that:

a) enable Customer to access to the Cloud Console via self-managed passwords (with restrictions on minimum length and special characters);
b) perform automated monitoring of break-in attempts;
c) enable Customer to access the API via a unique access key which Customer can generate, regenerate, and expire;
d) record Customer actions through the API and Cloud Console providing the basis for investigation of incident management.

3. Security of Data

Docmosis shall ensure that:

a) all communication with the Cloud Services API must be SSL encrypted;
b) templates and other uploaded content are stored encrypted at rest;
c) any Personal Data sent to the Services and any generated documents, once processing is complete and delivery is attempted, are automatically and immediately deleted;
d) email is dispatched using transport layer security;
e) processing of data is geographically bound based on the processing location selected by the Customer;
f) templates and other uploaded content are stored in areas with role-based access.

4. Availability and Resilience

Docmosis shall:

a) monitor the availability and performance of Cloud Services every 60 seconds with deep-tests checking that generation of the test documents is successful;
b) engineer the Cloud Services to survive multiple points of failure, degrade in a predictable manner and remain as operational as possible, even in the event of core systems failures;
c) maintain multiple independent backup systems providing case-specific recovery options;
d) perform minor software updates to the Cloud Services as needed on the service and provide status notifications via: https://www.docmosis.com/status.

5. Regular Evaluation and Assessment

Docmosis shall:

a) continually evaluate the security of the Services to determine whether additional or different security measures are required;
b) engage an independent third-party to perform penetration testing of the Services.

6. Staff Practices

Docmosis shall:

a) require Docmosis employees to read and sign a confidentiality agreement which explains the importance and sensitivity of Personal Data;
b) ensure that employees of Docmosis can only access Cloud Services infrastructure by two factor authentication;
c) limit access of Docmosis employees to Cloud Services infrastructure to that necessary to execute the assigned roles.

Schedule 3

Subprocessors

Docmosis uses a range of third party Subprocessors to assist in providing the Services. These Subprocessors are set our below.

The exact Subprocessor(s) used will depend on the Processing Location selected by Customer.

Subprocessor	Processing Location
A100 ROW GmbH	Germany
Amazon Data Services Ireland Limited	Ireland

Schedule 4

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) 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.

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, 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 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

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

Clause 5 - Optional

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (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 purposes of processing and the risks involved for the data subjects.

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

7.5. Sensitive data

If the processing 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 ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

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

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit 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 an audit, the controller may take into account relevant certifications held by the processor.

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

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the

processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

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

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

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

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

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

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I LIST OF PARTIES

As specified in Schedule 1 of the Addenedum.

ANNEX II: DESCRIPTION OF THE PROCESSING

As specified in Schedule 1 of the Addenedum.

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

As specified in Schedule 2 of the Addenedum.

ANNEX IV: LIST OF SUB-PROCESSORS

As specified in Schedule 3 of the Addenedum.