Docmosis – Data Processing Addendum

This Data Processing Addendum ("**Addendum**") to the License Agreement, located at https://www.docmosis.com/DLA (the "**Agreement**"), between: the Client identified in the signature block below ("**Client**") and Docmosis Pty Ltd **("Company")** 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 Client Personal Data; and (b) any other applicable law which applies to any Client Personal Data;

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

1.1.3 "**Contracted Processor**" means Company 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means the GDPR, and any domestic legislation of each Member State implementing the GDPR, as amended, replaced or superseded from time to time;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 2016/679 of the European Parliament and of the Council 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 "**Restricted Transfer**" means:

1.1.8.1 a transfer of Client Personal Data from the Client to a Contracted Processor; or

1.1.8.2 an onward transfer of Client Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses;

1.1.9 "**Services**" means the Cloud Services and other activities to be supplied to or carried out by or on behalf of Company to the Client pursuant to the Agreement;

1.1.10 "**Standard Contractual Clauses**" means the contractual clauses set out in Annex 4.

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

1.2 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.

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

2. Processing of Client Personal Data

2.1 Company shall:

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

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

2.1.3 In the event of a Restricted Transfer occurring between the Client and the Company, ensure that the Standard Contractual Clauses in Annexure 4 are complied with.

2.2 The Client:

2.2.1 instructs Company (and authorises Company to instruct each Subprocessor) to:

2.2.1.1 Process Client Personal Data; and

2.2.1.2 in particular, transfer Client Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Agreement.

2.3 The Client agrees that this Addendum is Client's complete and final instructions to Company in relation to processing Client Personal Data.

2.4 Annex 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of Client 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 Company and Client on additional instructions for processing,

including agreement on any additional fees Client will pay to Company for carrying out such instructions. Client may terminate this Addendum if Company declines to follow instructions requested by Client that are outside the scope of this Addendum. Nothing in Annex 1 (including as amended pursuant to this section 2.4) confers any right or imposes any obligation on any party to this Addendum.

3. Company Personnel

Company shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to Client Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Client 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, Company shall in relation to Client Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, in accordance with Company's security standards described in Annex 2 **("Security Measures")**.

4.2 Client is responsible for reviewing the information made available by Company relating to data security and making an independent determination as to whether the Services meet Client's requirements and legal obligations under Data Protection Laws. Client acknowledges that the Security Measures are subject to technical progress and development and that Company 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 Client.

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

5. Subprocessing

5.1 The Subprocessors currently engaged by Company and authorized by Client are listed in Annex 3. The Client generally authorises Company 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 Company may continue to use those Subprocessors already engaged by Company as at the date of this Addendum, subject to Company in each case as soon as practicable meeting the obligations set out in section 5.4.

5.3 Company shall give Client 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, Client notifies Company in writing of any objections (on reasonable grounds) to the proposed appointment Client may by written notice to Company 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 Client's sole and exclusive remedy if Client objects to any new Third Party Subprocessor.

5.4 With respect to each Subprocessor, Company shall:

5.4.1 before the Subprocessor first Processes Client 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 Client Personal Data required by the Agreement;

5.4.2 ensure that the arrangement between on the one hand (a) Company, 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 Client Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;

5.4.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) Company, or (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Client Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the Client; and

5.4.4 provide to Client 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 Client may request from time to time.

5.5 Company shall ensure that each Subprocessor performs the obligations under sections 2.1, 3, 4, 6.1, 7.2, 8 and 10.1, as they apply to Processing of Client Personal Data carried out by that Subprocessor, as if it were party to this Addendum in place of Company.

6. Data Subject Rights

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

6.2 Company shall:

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

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

7. Personal Data Breach

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

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

7.3 Company's notification of or response to a Personal Data Breach under this section 7 will not be construed as an acknowledgement by Company of any fault or liability with respect to the Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Company shall provide commercially reasonable assistance to the Client with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Client 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 Client Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Client Personal Data

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

9.2 Subject to section 9.3 Company 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 Client Personal Data.

9.3 Each Contracted Processor may retain Client 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 Company shall ensure the confidentiality of all such Client Personal Data and shall ensure that such Client Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

10. Audit rights

10.1 If the GDPR applies to the processing of Client Personal Data, and subject to sections 10.2 to 10.7, Company shall make available to the Client on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by Client or an auditor mandated by Client in relation to the Processing of Client Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Client only arise under section 10.1 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).

10.3 Following receipt by Company of a request under section 10.1, Company and Client 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 10.1.

10.4 Company may charge a fee (based on Company's reasonable costs) for any audit under section 10.1. Company will provide Client with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Client will be responsible for any fees charged by any auditor appointed by Client to conduct any such audit.

10.5 Company may object in writing to an auditor appointed by Client to conduct any audit under section 10.1 if the auditor is, in Company's reasonable opinion, not suitably qualified or independent, a competitor of Company or otherwise manifestly unsuitable. Any such objection by Company will require Client to appoint another auditor or conduct the audit itself.

10.6 Client undertaking an audit under section 10.1 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.

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

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

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

10.7.3 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:

10.7.3.1 Client undertaking an audit reasonably considers necessary because of genuine concerns as to Company's compliance with this Addendum; or

10.7.3.2 Client 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 Client undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Company of the audit or inspection.

11. General Terms

Governing law and jurisdiction

11.1 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

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

11.3 Subject to section 11.2, 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

11.4 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.

Signature : _____

Name : _____

Position : _____

On behalf of Client: _____

Date Signed : _____

Signature : _____

Name : _____

Position : _____

On behalf of Company: **Docmosis Pty Ltd.**

Date Signed : _____

Annex 1: Details of Processing of Client Personal Data

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

Subject matter of the Processing of Client Personal Data

The subject matter of the Processing of the Client Personal Data are set out in the Agreement and this Addendum.

Duration of the Processing of Client Personal Data

The Processing will begin on the Client sending the Client Data including the Client Personal Data to the Services and will end once the generated document and any Client Personal Data is deleted.

The nature and purpose of the Processing of Client Personal Data

Client may submit Personal Data to Company's Service, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to Client's clients' Personal Data and other Personal Data concerning Client's employees, contractors, collaborators, customers, prospects, suppliers and subcontractors.

Company provides cloud based document generation services. Client, as a client of Company, may use the Services to generate documents. Company has no control over whether the data sent to be Processed by the Services is in fact Client Personal Data.

If Client sends Client Personal Data to be Processed by the Services then the generated document may then contain Client Personal Data.

Once the Client Personal has been Processed and any generated document has been returned to the Client, the generated document and any Client Personal Data is automatically deleted from the Company's systems (including that of its Subprocessor).

The types of Client Personal Data to be Processed

Client has complete control over the types of Client Personal Data it sends to be Processed by the Services. Company has no way of knowing if the types of data sent to be Processed by the Services are in fact Client Personal Data.

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

Client has complete control over the categories of Data Subject Personal Data it sends to be Processed by the Services. Company has no way of knowing the categories of Data Subject Personal Data sent to be Processed by the Services.

The obligations and rights of Client

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

Client shall follow the "Guidelines for Using the Docmosis Cloud Services in a GDPR-Compliant Manner" issued by the Company (dated 21 Oct 2019 and as amended or updated).

Annex 2: Security Measures

As from the Effective Date, Company will implement and maintain the security measures set out below (as updated from time to time in accordance with section 4.2 of this Addendum).

1. Physical Security

1.1. Processing occurs entirely on Amazon Web Services (AWS) infrastructure. This provides comprehensive physical security as well as providing the facilities supporting the non-physical system security.
1.2. The Company premises has physical access control systems and is protected after hours by an externally monitored security system. The local computer network has multiple layers of network devices to protect against external threats.

2. System Security

2.1. Client accesses the Services via self-managed passwords (restrictions on minimum length and special characters) with monitoring and notifications to Company of break-in attempts.
2.2. API access requires a unique access key which Client can rotate and expire.
2.3. Client actions are audited providing the basis for investigation of incident management.
2.4. Employee access to cloud infrastructure is controlled by two factor authentication.

3. Security of Data

3.1. Transport Encryption - All communication with the Services is SSL encrypted.
3.2. At Rest Encryption - Templates and other uploaded content and are encrypted at rest.
3.3. “Short Memory" Data Retention – Client Personal Data and the generated documents are delivered then automatically and immediately deleted.
3.4. Email Security - email is dispatched using transport layer security (SMTP TLS).
3.5. Processing of data and generated documents is geographically bound (either USA or EEA) within the region selected by the Client.
3.6. Data (templates and other uploaded content) are stored in areas with role-based access and access by employees requires interaction with access-control systems.

4. Availability and Resilience

4.1. High Availability Architecture - Load balanced, high-performance, redundant and monitored 24/7.
4.2. Monitoring – Company uses publicly visible third party systems to monitor the availability and performance of Services. Key API end points are monitored every 60 seconds with deep-tests checking the contents of the generated test documents. Historical uptime results can be viewed here: https://www.docmosis.com/monitoring
4.3. Strong Software Design - The service is engineered 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.
4.4. Backed up - Multiple independent backup systems in place providing case-specific recovery options.

4.5. Version Controlled – Templates and other uploaded content are version controlled and can be reverted and restored on an as-needs basis.
4.6. Service Status – Minor software updates are performed as needed on the service. Status notifications are available here: https://www.docmosis.com/status

5. Regular Evaluation and Assessment

5.1. Company continually evaluates the security of its Services to determine whether additional or different security measures are required.

6. Staff Practices

6.1. Employee access to infrastructure and data is limited to that necessary to execute the assigned roles. Data is stored in areas with role-based access.
6.2. Employees are required to read and sign a confidentiality agreement which explains the importance and sensitivity of Client Personal Data.
6.3. The Company provides ongoing training to employees on the importance of security and their compliance with the Company Password Policy and Acceptable Use of IT Policy.

Annex 3: Subprocessors

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

Subprocessor	Type of Service
Amazon Web Services	Cloud hosting services.

ANNEX 4

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Address:

Tel.: .....; fax: ..... ; e-mail: .....

Other information needed to identify the organisation:

(the data **exporter**)

And

Name of the data importing organisation:. **Docmosis Pty Ltd**

Address: **Suite 8 / 5 Hasler Rd, Osborne Park, WA 6154 Australia**

Tel.: **+61 8 6111 0559**; e-mail:**admin@docmosis.com**

Other information needed to identify the organisation:

ACN 163 331 413

(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

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

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

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

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

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

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

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

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

(ii) any accidental or unauthorised access, and

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

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

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

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

---

2 Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

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

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

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

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

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

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

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

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

---

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

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

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

Clause 12

Obligation after the termination of personal data processing services

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

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

On behalf of the data exporter:
Name (written out in full):
Position:
Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

On behalf of the data importer:
Name (written out in full): Docmosis Pty Ltd.
Position:
Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is: _____

Data importer

The data importer is: **Docmosis Pty Ltd.**

Data subjects

Data Exporter may submit Personal Data to Data Importer's Service, the extent of which is determined and controlled by Data Exporter in its sole discretion, and which may include, but is not limited to Data Exporter's clients' Personal Data and other Personal Data concerning Data Exporter's employees, contractors, collaborators, customers, prospects, suppliers and subcontractors.

Categories of data

Data Exporter has complete control over the categories of Personal Data it sends to be Processed by the Services. Data Importer has no way of knowing the categories of Personal Data sent to be Processed by the Services.

Special categories of data (if appropriate)

Data Exporter has complete control over the special categories of Personal Data it sends to be Processed by the Services. Data Importer has no way of knowing the special categories of Personal Data sent to be Processed by the Services.

Processing operations

Data Importer provides cloud based document generation services. Data Exporter, as a client of Data Importer, may use the Services to generate documents. Data Importer has no control over whether the data sent to be Processed by the Services is in fact Client Personal Data.

If Data Exporter sends Client Personal Data to be Processed by the Services then the generated document may then contain Client Personal Data.

Once the Client Personal Data has been Processed and any generated document has been returned to the Client, the generated document and any Client Personal Data is automatically deleted from the Data Importer's systems (including that of its Subprocessor).

Client shall follow the "Guidelines for Using the Docmosis Cloud Services in a GDPR-Compliant Manner" issued by the Company dated 25 May 2018 and as amended or updated.

DATA EXPORTER

Name:……

Authorised Signature ……

DATA IMPORTER

Name:……

Authorised Signature ……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Annex 2