Data Protection Addendum

Last updated: November 1, 2021

This Data Protection Addendum ("DPA") is incorporated into and made part of the Terms of Service ("Terms") and governs the processing of personal data by DocuX as a Processor on behalf of Customer. This DPA shall be effective on or later of (i) the effective date of the Terms; or (ii) the date both parties execute this DPA in accordance with Section 1 below ('Effective Date'). Unless otherwise defined in this DPA, capitalized terms shall have the same meaning as given to them in the Terms.

1. INSTRUCTIONS AND EFFECTIVENESS

a. This DPA has been pre-signed on behalf of DocuX. To enter into this DPA, Customer must (i) be a customer of DocuX Service; (ii) complete the signature below by signing and providing all relevant information; and (iii) submit the completed and signed DPA to us.

b. This DPA will only be effective if executed accurately and in full accordance with Section 1 and submitted to us. Where Customer makes any deletions or other revisions to this DPA, this DPA will be null and void.

c. Customer signatory represents to us that he or she has the legal authority to bind Customer and is lawfully able to enter into this DPA.

d. This DPA will terminate automatically upon termination of the Terms, unless earlier terminated pursuant to the terms of this DPA.

2. DEFINITIONS

a. "Data Protection Law" means European Data Protection Law or US Data Protection Law or Brazil LGPD or Singapore PDPA or any other data protection law legislated in any other country that are applicable to the processing of Customer Personal Data;

b. "Brazil LGPD" means regulations approved as Law No. 13.709 of 14 August 2018, General Personal Data Protection Law ('LGPD'), which was further amended by Law No. 13.853 of 8 July 2019 which came into effect from September 18, 2020.

c. "Controller", "Processor", "Subprocessor", "Data Subject", "Personal Data", "Process" and "Processing", shall have the same meaning as ascribed to them under the European Data Protection Law.

d. "Customer Personal Data" means any personal data provided by Customer to DocuX in connection with DocuX Services.

e. "Data Protection Officer" means a data protection officer appointed pursuant to Data Protection Law.

f. "EEA" means European Economic Area;

g. "European Data Protection Law" means : (i) 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 (General Data Protection Regulation) (the "EU GDPR"); (ii) in respect of the United Kingdom the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "UK GDPR"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) the Swiss Federal Data Protection Act ("Swiss DPA").

h. "Restricted Transfer" means: (i) where the EU GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not subject based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; (iii) where the Swiss DPA applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner; (iv) where the Singapore PDPA applies, a transfer of personal data to a country outside of Singapore which does not accord a standard of protection that is comparable to that under the PDPA; or (v) where the Brazil LGPD applies, a transfer of personal data to a country outside of Brazil that does not provide for adequate level of protection of personal data.

i. "Singapore PDPA" means the Personal Data Protection Act 2012 (No.26 of 2012) including the subsequent amendments.

j. "Standard Contractual Clauses" means (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs"); (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR ("UK SCCs"); and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner (the "Swiss SCCs").

k. "Security Incident" means any confirmed unauthorized or unlawful breach of the security that leads to accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of or access to Customer Personal Data processed by DocuX and/or its Subprocessors in connection with provision of DocuX Services. For removal of doubts, Security Incident shall not include unsuccessful attempts or activities that do not compromise the security of personal data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks or firewalls or networked systems.

l. "Sensitive Information" means Personal Information revealing a Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation.

m. "US Data Protection Law" means all data protection or privacy laws and regulations applicable to the Customer Personal Data in question in force within the United States, including the California Consumer Privacy Act (as may be amended from time to time) (the "CCPA"), and any rules or regulations implementing the foregoing.

3. RELATIONSHIP OF THE PARTIES

Where applicable Data Protection Law provides for the roles of "controller," "processor," and "subprocessor":

a. Where you are a controller of the personal data covered by this DPA, we shall be a processor processing personal data on your behalf and this DPA shall apply accordingly;
b. Where you are a processor of the personal data covered by this DPA, we shall be a Subprocessor of the personal data and this DPA shall apply accordingly; and
c. Where and to the extent we process personal data as a controller, we will process such personal data in compliance with applicable Data Protection Laws and only Sections 11 and 4(e) of this DPA, to the extent applicable.

4. DATA PROCESSING

b. DocuX shall:
   (i) Process Customer Personal Data for the legitimate business purpose only and/or to provide DocuX Services.
   (ii) Process Customer Personal Data only in accordance with the specific instructions of the Customer or Permitted Users unless Processing is required by applicable laws. Such instructions can be in writing or by electronic means.
   (iii) Comply with all applicable Data Protection Laws in the Processing of Customer Personal Data

c. Each Customer or Permitted User hereby instructs and authorizes DocuX (and authorizes DocuX to instruct each Subprocessor) to Process Customer Personal Data and Account-Related Information for the above purposes including authorizing DocuX to transfer such data to any country or territory as reasonably necessary for the provision of DocuX Services and consistent with the Terms.

d. You will be responsible for providing or making Customer Personal Data available to us in compliance with the Data Protection Law, including providing any necessary notices to, and obtaining any necessary consents from, Data Subjects whose Personal Data is provided by you to us for Processing pursuant to this DPA. You acknowledge that DocuX Service is not intended or designed for the Processing of Sensitive Information, and you agree not to provide any Sensitive Information through the Service. The parties agree that you provide Customer Personal Data to us as a condition precedent to our performance of the DocuX Service and that Customer Personal Data is not exchanged for monetary or other valuable consideration. You acknowledge that we are an independent controller when carrying out any activities not related solely to our Processing of Customer Personal Data added by you to the Service.

e. You acknowledge and agree that as part of providing DocuX Services, we has the right to use data relating to or obtained in connection with the operation, support or use of the DocuX Service for our legitimate internal business purposes, such as to support billing processes, to administer DocuX Service, to improve, benchmark, and develop our products and services, to comply with applicable laws (including law enforcement requests), to ensure the security of DocuX Service and to prevent fraud or mitigate risk. To the extent any such data is personal data, we warrant and agree that:
   (i) we will process such personal data in compliance with applicable Data Protection Law and only for the purposes that are compatible with those described in this Section 3; and
   (ii) we will not use such personal data for any other purpose or disclose it externally unless we have first aggregated and anonymized the data, so it does not identify you or any other person or entity.

5. OUR PERSONNEL

We shall take reasonable steps to ensure the reliability of all our employees who have access to Customer Personal Data and Account-Related Information and to ensure that such employees have committed themselves to a binding duty of confidentiality in respect of such Personal Data and Account-Related Information.

6. PARTIES' OBLIGATIONS

a. We shall:
   (i) Make copies of the Account-Related Information and Customer Personal Data only to the extent reasonably necessary for the provision of DocuX Services (which, for clarity, may include generating logs, back-up, mirroring and other similar techniques, security, disaster recovery, testing of DocuX Services).
   (ii) Retain all Account-Related Information and Customer Personal Data during the validity of the Subscription Term and as per the Subscription Plan purchased by you. In case of Termination for any reason, unless otherwise agreed, we may, at our sole discretion, delete all or part of the Account-Related Information and Customer Personal Data within such time as we may deem appropriate.
   (iii) Provide copy of all Account-Related Information and Customer Personal Data held by us to you or Permitted Users in a commonly used format and medium.
   (iv) Obtain your prior written approval before using or making available any Account-Related Information or Customer Personal Data other than as provided for in the Terms.
   (v) Attempt to redirect the law enforcement agency to you if a law enforcement agency sends us a demand for Customer Personal Data (e.g., a subpoena or court order). As part of this effort, we may provide your contact information to the law enforcement agency. If compelled to disclose Customer Personal Data to a law enforcement agency, then we will give you reasonable notice of the demand to allow you to seek a protective order or other appropriate remedy to the extent we are legally permitted to do so.

b. You acknowledge that we are under no duty to investigate or ensure the completeness, accuracy or sufficiency of (i) any instructions received from you or (ii) any Account-Related Information or Customer Personal Data.

c. You will:
   (i) Ensure that you are entitled to transfer Account-Related Information and Customer Personal Data to us so that we may lawfully process and transfer the said information in accordance with the Terms and this DPA;
   (ii) Ensure that the Account-Related Information or Customer Personal Data sent to us for Processing pursuant to the Terms and this DPA is accurate, updated, adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
   (iii) Ensure that relevant Data Subjects have been informed of, and have given their consent to, such use, processing and transfer as required under Data Protection Law;
   (iv) Notify us in writing about delay or any situation or development that shall in any way influence, change or limit our ability to process Account-Related Information or Customer Personal Data as set out in the Terms and this DPA;

7. SECURITY & AUDIT

a. We shall, in accordance with requirements under the Data Protection Law, implement appropriate technical and organizational measures to safeguard the Account-Related Information and Customer Personal Data from unauthorized or unlawful Processing, or accidental loss, alteration, disclosure, destruction or damage, and that, having regard to the state of technological development and the cost of implementing any measures. Such measures are described in Exhibit B to this DPA. Such measures shall be proportionate and reasonable to ensure a level of security appropriate to the harm that might result from the unauthorized or unlawful Processing or accidental loss, alteration, disclosure, destruction, or damage and to the nature of the Customer Personal Data to be protected.

b. We shall, in accordance with Data Protection Laws, make available to you such information in our possession or control as you may reasonably request with a view to demonstrating our compliance with the obligations of data processors under Data Protection Laws in relation to its processing of Customer Personal Data.

c. You may exercise its right of audit under Data Protection Laws in relation to Personal Information. Upon request, and on the condition that you have entered into an applicable non-disclosure agreement with us, we shall:
   (i) supply (on a confidential basis) a summary copy of our audit report(s) ("Report") to you, so you can verify our compliance with the audit standards against which we have been assessed; and
   (ii) provide written responses (on a confidential basis) to all reasonable requests for information made by you related to our Processing of Customer Personal Data, including responses to information security and audit questionnaires, that are necessary to confirm our compliance with this DPA, provided that you shall not exercise this right more than once per year.

d. Only to the extent you cannot reasonably satisfy our compliance with this DPA through the exercise of your rights above, where required by applicable Data Protection Law or the Standard Contractual Clauses, you and you authorized representatives may conduct audits (including inspections) during the term of the Terms to establish our compliance with the terms of this DPA, on the condition that you and your authorized representatives have entered into an applicable non-disclosure agreement with us and at your own cost. Notwithstanding the foregoing, any audit (or inspection) must be conducted during our regular business hours, with reasonable advance notice (which shall not be less than 30 days) and subject to reasonable confidentiality procedures. Such audit (or inspection) shall not require us to disclose to you or your authorized representatives, or to allow you or your authorized representatives to access:
   (i) any data or information of any other DocuX customer;
   (ii) our internal accounting or financial information;
   (iii) our trade secrets;
   (iv) any information that, in our reasonable opinion could: (1) compromise the security of our systems or premises; or (2) cause us to breach our obligations under applicable Data Protection Law or our security, confidentiality and or privacy obligations to any other DocuX customer or any third party; or
   (v) any information that you or your authorized representatives seek to access for any reason other than the good faith fulfilment of your obligations under the applicable Data Protection Law and our compliance with the terms of this DPA.

e. An audit or inspection permitted above shall be limited to once per year, unless (1) we have experienced a Security Incident within the prior of twelve (12) months which has impacted Customer Personal Data; or (2) you able to evidence an incidence of our material noncompliance with this DPA.

8. DATA SUBJECT RIGHTS AND REQUESTS

a. Taking into account the nature of the Processing, DocuX Service provides functionality to assist you by appropriate technical and organizational measures, insofar as this is possible, to access, correct, amend, restrict, or delete Customer Personal Data contained in DocuX Services to address requests by a Data Subject under the GDPR. To the extent you, in your use of DocuX Services, are not familiar with DocuX Services functionality that may be used for these purposes, we will provide you with additional Documentation or customer support assistance to educate you on how to take such actions.

b. We shall notify you as soon as reasonably practicable if we receive:
   (i) a request from a Data Subject for access to that person's Personal Data (relating to the DocuX Services);
   (ii) any communication from a Data Subject (relating to the DocuX Services) seeking to exercise rights conferred on the Data Subject by Data Protection Law in respect of Customer Personal Data; or
   (iii) any complaint or any claim for compensation arising from or relating to the Processing of such Customer Personal Data.

c. We shall not disclose the Customer Personal Data to any Data Subject or to a third party other than at your request, as provided for in this DPA, or as required by law in which case we shall to the extent permitted by law inform you of that legal requirement before you disclose the Customer Personal Data to any Data Subject or third party.

d. We shall not respond to any request from a Data Subject except on the documented instructions of yours or a Permitted User or as required by law, in which case we shall to the extent permitted by law inform you of legal requirement before we respond to the request.

9. SECURITY INCIDENT REPORTING

a. We shall notify you without undue delay upon we or any Subprocessor becoming aware of a Security Incident, providing you with the sufficient information to allow you to meet any obligations to report or inform (a) affected Data Subjects, and (b) any other persons or entities required to be recipients of a notification, of the Security Incident.

b. We shall use reasonable efforts to cooperate with you and take such commercially reasonable steps as are directed by you to assist in the investigation, mitigation, and remediation of each such Security Incident. Our notification of or response to a Security Incident in accordance with this DPA will not be construed as an acknowledgement by us of any fault or liability in respect of such Security Incident.

10. RETURN OR DISPOSAL

Prior to or upon termination or expiration of the Terms for any reason, we may retrieve Customer Personal Data processed by DocuX Services in accordance with the Terms at your request provided in writing to us. We shall, as soon as possible, return or delete Customer Personal Data from DocuX Services, unless applicable law requires storage of the Customer Personal Data.

11. RESTRICTED TRANSFERS

In connection with the performance of the Terms and this DPA, you authorize us to transfer Personal Information internationally, and in particular to locations outside of the United Kingdom and EEA, Brazil, Singapore, such as the United States as the case may be. The parties agree that when the transfer of Customer Personal Data from you (as "data exporter") to us (as "data importer") is a Restricted Transfer and applicable Data Protection Law requires that appropriate safeguards are put in place and if required, it shall be subject to the appropriate Standard Contractual Clauses, which shall be deemed incorporated into and form a part of this DPA, as follows:

a. In relation to transfers of Customer Personal Data protected by EU GDPR and processed in accordance with Section 3(a)(i) and 3(a)(ii) of this DPA, the EU SCCs shall apply completed as under:
   (i) Module Two or Module Three will apply as applicable;
   (ii) In Clause 7, the optional docking clause will apply;
   (iii) In Clause 9, Optional 2 shall apply, along with the time periods mentioned in the Section 12(b) in regard to Subprocessor changes;
   (iv) In Clause 11, the optional language will not apply;
   (v) In Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;
   (vi) In Clause 18(b), disputes shall be resolved before the courts of Ireland;
   (vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Exhibit A to this DPA, as applicable; and
   (viii) Subject to Section 7 of this DPA, Annex II of the EU SCCs shall be deemed completed with the information as set out in Exhibit B to this DPA;

b. In relation to transfers of Customer Personal Data protected by EU GDPR and processed in accordance with Section 3(a)(iii) of this DPA, the EU SCCs shall apply completed as under:
   (i) Module One will apply;
   (ii) In Clause 7, the optional docking clause will apply;
   (iii) In Clause 11, the optional language will not apply;
   (iv) In Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;
   (v) In Clause 18(b), disputes shall be resolved before the courts of Ireland;
   (vi) Annex I of the EU SCCs shall be deemed completed with the information set out in Exhibit A to this DPA, as applicable; and
   (vii) Subject to Section 7 of this DPA, Annex II of the EU SCCs shall be deemed completed with the information as set out in Exhibit B to this DPA;

c. In relation to transfers of Customer Personal Data protected by UK GDPR, the EU SCCs will also apply in accordance with paragraphs (a) and (b) above with the following modifications:
   (i) any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the UK GDPR; references to specific Articles of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK GDPR;
   (ii) references to "EU", "Union" and "Member State law" are all replaced with "UK"; Clause 13(a) and Part C of Annex I of the EU SCCs are not used; references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the Information Commissioner and the courts of England and Wales;
   (iii) Clause 17 of the EU SCCs is replaced to state that "The Clauses are governed by the laws of England and Wales" and Clause 18 of the EU SCCs is replaced to state "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceeding against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts",

   unless the EU SCCs, implemented as described above, cannot be used to lawfully transfer such Customer Personal Data in compliance with the UK GDPR in which case the UK SCCs shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant Annexes or Appendices of the UK SCCs shall be populated using the information contained in Exhibits A and B of this DPA (as applicable);

d. In relation to transfers of Customer Personal Data protected by Swiss DPA, the EU SCCs will also apply in accordance with paragraphs (a) and (b) above with the following modifications:
   (i) any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;
   (ii) references to “EU”, “Union”, “Member State” and “Member State law” shall be interpreted as references to Switzerland, Swiss law, as the case may be; and
   (iii) references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the Swiss Federal Data Protection and Information Commissioner and competent courts in Switzerland,

unless the EU SCCs, implemented as described above, cannot be used to lawfully transfer such Customer Personal Data in compliance with the Swiss DPA in which case the Swiss SCCs shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant Annexes or Appendices of the Swiss SCCs shall be populated using the information contained in Exhibits A and B to this DPA (as applicable);

e. It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Terms (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict.

12. SUBPROCESSORS

a. You agree that we may engage Subprocessors to process Customer Personal Data on your behalf. The Subprocessors currently engaged by us and authorised by you are listed at https://www.docux.ai/legal/subprocessors.html. With respect to each Subprocessor, we shall,
   (i) before the Subprocessor first Processes Customer Personal Data, 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 Terms and this DPA;
   (ii) ensure that the arrangement between DocuX, or its Affiliate or the relevant intermediate Subprocessor, and 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 DPA; and
   (iii) remain fully responsible to you for the performance of such Subprocessor's data protection obligations under such terms.

b. We will inform you of any intended changes concerning the addition or replacement of Subprocessors by updating our above webpage, which you acknowledge is your responsibility to check regularly. You may object to such changes on reasonable grounds of data protection within ten (5) business days after being notified of the engagement of the Subprocessor. If you object to a new Subprocessor, as permitted in the preceding sentence, we will use reasonable efforts to make available to you a change in DocuX Service or recommend a commercially reasonable change to your configuration or use of the DocuX Service to avoid Processing of Customer Personal Data by the objected-to new Subprocessor. If we are unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, either party may terminate the component of the DocuX Service which cannot be provided by us without the use of the objected-to new Subprocessor by providing written notice to the other party. We will refund you any prepaid fees covering the remainder of the term of your subscription following the effective date of termination with respect to such terminated component of the DocuX Service, without imposing any penalty for such termination on you.

13. GENERAL

a. The parties agree that this DPA shall replace any existing DPA the parties may have previously entered into in connection with DocuX Services.

b. Except for the changes made by this DPA, the Terms remains unchanged and in full force and effect. If there is any conflict between this DPA and the Terms, this DPA shall prevail to the extent of that conflict in connection with the processing of Customer Personal Data. If there if any conflict between the Standard Contractual Clauses and the Terms (including this DPA), the Standard Contractual Clauses shall prevail to the extent of that conflict in connection with the processing of Customer Personal Data.

c. Notwithstanding anything to the contrary in the Terms or this DPA, the liability of each party and each party's affiliates under this DPA shall be subject to the exclusions and limitations of liability set out in the Terms.

d. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Terms, unless required otherwise by applicable Data Protection Laws.

e. This DPA and the Standard Contractual Clauses will terminate simultaneously and automatically with the termination or expiry of the Terms.

Customer signatures	**DocuX signatures**
	
_____	_____
Customer Name:	For DocuX, Inc.,
Name of the signatory:	Name of the signatory: Deepak Dhanak
Title:	Title: Authorized Signatory
Date:	Date: November 1, 2021
Data Protection Officer:	Data protection point of contact: Pankaj Minda
Contact of DPO:	Contact of DPO: legal@docux.ai

Exhibit A

Description of the Processing Activities / Transfer

Annex 1(A) List of parties:

	Data Exporter	**Data Importer**
Name	**Customer**	**DocuX, Inc.**
Address / Email Address	As provided in the DPA	As provided in the DPA
Contact person's name position and contact details	As provided in the DPA	As provided in the DPA
Activities relevant to the transfer	Please see Annex 1(B) below	Please see Annex 1(B) below
Role	Please see Annex 1(B) below	Please see Annex 1(B) below

Annex 1(B) Description of Processing / Transfer:

The parties acknowledge that DocuX's processing of personal data will include all personal data submitted or uploaded to the DocuX Services by you from time to time, for the purpose of, or otherwise in connection with, DocuX providing the DocuX Services to you. Set out below are descriptions of the processing/transfers of personal data as contemplated as of the date of this DPA. Such descriptions are subject to change or may be supplemented pursuant to the Section 3 of this DPA.

Categories of data subjects	Customer, Permitted Users and Customer's collaborators
Categories of personal data transferred	Data exporter may submit Personal Information to DocuX Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following Personal Information : First and Last Name, Email Address, Address, Phone Number, Screen name / Handle, Credit Card Information, Job Title, IP Address, API Key, User Identifiers, Password, Cookies, Time Zone, About me, Avatar or Actual Image, Device information, Employment Information, Personal data in User Generated Content, electronic signature, digital signature
Controller / Processor roles	Controller (Customer) to Processor (DocuX)
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	Providing DocuX Services (creation, collaboration, conclusion, control and analysis of documents and contracts) and account management related processing pursuant to Terms of Service
Purpose of the data transfer	Performance of DocuX Services pursuant to Terms of Service
Duration of processing	For the duration of the Terms of Service

* * * * * * *

Exhibit B

Technical and Organizational Security Measures

DocuX will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Information uploaded to DocuX Service, as described in this Exhibit. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the DPA.

A. SECURITY GOVERNANCE

We maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to:

(a) help our customers secure their data processed using our online products and services against accidental or unlawful loss, access, or disclosure,

(b) identify reasonably foreseeable and internal risks to security and unauthorised access to our online products and services, and

(c) minimize security risks, including through risk assessment and regular testing.

Our Chief Technology Officer coordinates and is primarily responsible for the company's information security program.

Such program covers the following core functions:

- Application security (secure development, security feature design, and secure development training)
- Infrastructure security (data centers, cloud security, and strong authentication)
- Monitoring and incident response
- Vulnerability management
- Compliance and technical privacy
- Security awareness (onboarding training and awareness campaigns)

B. ACCESS CONTROL

(a) Preventing unauthorized product access

Third party data hosting and processing: DocuX Service are hosted with third party cloud infrastructure providers. We maintain contractual relationships with these vendors in accordance with this DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: DocuX Service infrastructure is hosted with multi-tenant, outsourced infrastructure providers. Their physical and environmental security controls are audited for SOC 2 Type I, II, and III, and ISO 27001 compliance, among other certifications.

Authentication: Customers who interact with DocuX Services via the user interface are required to authenticate before they are able to access their non-public data.

Authorization: Customer Content and Customer Personal Data is stored in multi-tenant storage systems which are only accessible to our Customers via application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model is designed to ensure that only the appropriately assigned individuals can access relevant data, features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

(b) Preventing unauthorized product use

We implement industry standard access controls and detection capabilities for the internal networks that support our platform.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure.

Static code analysis: Automated security reviews of code stored in our source code repositories, performed through static code analysis, checking for coding best practices and identifiable software vulnerabilities.

Penetration testing: We maintain relationships with industry recognized penetration testing service providers for annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

Bug bounty: A bug bounty program invites and incentivizes independent security researchers to ethically discover and disclose security flaws. We implement a bug bounty program in an effort to widen the available opportunities to engage with the security community and improve the product defenses against sophisticated attacks.

(c) Limitations of privilege and authorization requirements

Product access: Only a subset of our personnel has access to the products and to customer data on need-to-know basis via controlled interfaces. The intent of providing access to a subset of personnel is to provide effective customer support, troubleshoot potential problems, detect, and respond to security incidents, and implement data security. We actively discourage access to platform and customer data by our personnel unless absolutely necessary.

Personnel Security: Our personnel are required to conduct themselves in a manner consistent with our guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. We conduct reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local law and regulations.

All our personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, our confidentiality and security policies. Personnel are provided with security training.

C. ENCRYPTION

In-transit: ALL customer data in DocuX Services is encrypted in transit over public networks to protect it from unauthorized disclosure or modification. Our implementation of TLS enforces the use of strong ciphers and key-lengths wherever supported by the browser.

At-rest: Data drives holding customer data and attachments use industry-standard AES-256 encryption at rest.

D. INPUT CONTROLS

Detection: We have designed our infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregate log data and alert appropriate personnel of malicious, unintended, or anomalous activities. Our personnel are responsive to known incidents.

Response and tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize product and customer damage or unauthorized disclosure. Notifications will be in accordance with the terms of the Terms.

E. DATA DELETION AND PORTABILITY

We enable customers to manage their own account and data including delete or export their account data in a manner consistent with the functionality of DocuX Services. Instructions and related details are provided within the applicable functionality within the DocuX Services.

F. AVAILABILITY CONTROLS

Our products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists our operations in maintaining and updating the product applications and backend while limiting downtime.

Redundancy: The infrastructure providers use designs to eliminate single points of failure and minimize the impact of anticipated environmental risks. Our platform is designed to allow us to perform certain types of preventative and corrective maintenance without interruption.

Business Continuity: We have designed and regularly plan and test our business continuity planning/disaster recovery programs.

* * * * * * *