1. Interpretation

1.1 Definitions used in these Terms of Use are defined in clause 13 (Definitions and Interpretation) or the relevant Schedules.

2. Access to Cloud Based Technology

2.1 Subject to the receipt of the relevant Access Fees, the Company will provide access to the Cloud Based Technology (**"Access"**) from the Start Date during the Term. The Customer may only access the Cloud Based Technology for its own business purposes.

2.2 The Customer shall comply with these Terms of Use, any terms of use or service (including the acceptable use policy set out in the Acceptable Use Schedule) and privacy and/or cookies policy that the Company may provide to Customer or publish online on its Website, all of which are incorporated into these Terms of Use by reference.

2.3 The Company shall provide Access Methods, through which the Customer can access the Cloud Based Technology. The Company grants the Customer a non-exclusive right to use the Access Methods for the purposes of accessing the Cloud Based Technology, and integrating it into the Customer's automation workflows via API calls during the Term.

2.4 The Company shall provide Access with reasonable skill and care and will comply with applicable laws and regulations with respect to its activities under these Terms of Use.

2.5 If the Company agrees to provide any additional services to Customer these will be set out in a separate agreement.

2.6 The Customer is responsible for determining if the Cloud Based Technology and Access meet its needs, expectations and requirements. The Company:

(a) does not warrant that the Customer's use of or access to the Cloud Based Technology will be uninterrupted or error-free;

(b) is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, and the Customer acknowledges that the Cloud Based Technology and the Access may be subject to limitations, delays and other problems inherent in the use of such communications facilities; and

(c) makes no warranties or other assurances as to the fitness for purpose of the Cloud Based Technology or Access or any Company Content.

2.7 All other conditions, warranties or other terms which might be implied or incorporated into these Terms of Use are excluded to the fullest extent permitted by law, including any implied conditions, warranties or other terms as to the satisfactory quality and fitness for purpose.

3. Free Trials, Access Orders, Access Fees and Service Levels

3.1 The Customer may request a free trial to evaluate the Cloud Based Technology, which shall last for 30 days from the date the Company confirms the Free Trial has commenced (**"Free Trial Term"**) and which shall be governed by these Terms of Use (**"Free Trial"**). During the Free Trial Term, the Customer may make such use of the Cloud Based Technology as is reasonably required in order to evaluate it for future use in its business, but not for any other purpose (including for business and/or commercial use). The Company reserves the right to suspend, limit or extend a Free Trial at any time in its sole discretion. On expiry of the Free Trial Term, access to the Cloud Based Technology will no longer be possible (but the parties may subsequently enter into an Access Order). One Free Trial per Customer is allowed and subsequent Free Trial requests may be rejected by the Company. No fees shall be payable during the Free Trial Term.

3.2 The Company and Customer may enter into Access Orders (in respect of a Proof of Concept or standard Access) in the manner and form provided by the Company upon request and which may be executed electronically.

3.3 An Access Order shall be entered into under and incorporate the terms of these Terms of Use. On valid execution of each Access Order the terms of that Access Order are incorporated into these Terms of Use and will not constitute a separate contractual relationship between the parties. No Access Order shall be valid or binding until properly executed by each of the Customer and the Company.

3.4 The Access order must set out the amount and frequency of any fees to be paid by the Customer (the "**Access Fees**").

3.5 All Access Fees must be paid in the manner and form set out in the relevant Access Order and clause 4. If the Access Fees are agreed to be paid in instalments this will not affect the Customer's obligation to pay the whole Access Fee, and any failure to pay an instalment when due will render the full annual Access Fees payable immediately.

3.6 The Access Fees may be increased during the Term if the Customer wishes to increase the maximum number of "documents" and/or otherwise increase the type or level of Access provided or in line with any other pricing mechanism agreed by the parties (in each case, as those terms are used in the relevant Access Order).

3.7 In addition to the fee changes set out in clause 3.6, the Company may increase the Access Fees at the end of the Term and end of each Renewal upon the Company giving at least 60 days' notice to Customer prior to the end of the Term or Renewal Term (as applicable) (the "**60 Day Period**").

3.8 For the avoidance of doubt, this clause 3 shall not apply where the Customer purchases the Access from the Reseller Partner rather than the Company.

4. Payment

4.1 All sums payable under and in accordance with these Terms of Use shall, save as agreed otherwise (e.g. credit card), be paid by electronic transfer to the Company's bank account or such bank account the Company may specify from time to time. Any charges on payments will be at the Customer's expense.

4.2 All sums payable under these Terms of Use are exclusive of VAT or other applicable sales tax which will be payable by the Customer, in addition to the sum in question, at the rate and in the manner prevailing at the relevant tax point and in the manner prescribed by law.

4.3 Unless otherwise agreed in the relevant Access Order, all sums due under these Terms of Use are payable in full with thirty (30) days, upon delivery of any invoice by the Company and without deduction, set off or withholding of any kind. In the event of any dispute as to the amount of an invoice, the Customer shall pay the amount in full pending the resolution of any dispute and the Company shall make any adjustment due immediately upon such resolution.

4.4 If any sums due under these Terms of Use are not paid when due the Company may charge interest in respect of those sums from the date due until payment is made in full (before and after any judgment) at 2% per annum over Barclays Bank Plc base rate from time to time accruing on a daily basis, and the Company may suspend the Customer's Access.

5. Customer's obligations

5.1 The Customer shall provide the Company with all necessary co-operation in relation to these Terms of Use and access to such information as may be required by the Company to provide Access. The Customer will be responsible for all activities that occur under the Customer's account.

5.2 The Customer will ensure that all users who access the Cloud Based Technology are aware of and comply with the terms and the policies referred to in clause 2.2 above, and will notify the Company immediately if it believes that there is any breach of

security such as the disclosure, theft or unauthorised use of any username or password, notify the Company immediately.

5.3 The Customer may not attempt to download, copy, modify, create derivative works from, frame, mirror, republish or distribute any portion of the Cloud Based Technology (but may use the Cloud Based Technology to operate embedded user interfaces and other similar features allowed by the Cloud Based Technology).

5.4 The Customer may only access the Cloud Based Technology for lawful purposes and may not process any data (including any Customer Data) illegally or in a manner which infringes the rights of any third party.

5.5 The Customer shall ensure that it takes all necessary steps to prevent any unauthorised access to, or use of, the Cloud Based Technology and notify the Company immediately of any such unauthorised access or use.

6. Intellectual Property Rights

6.1 The Customer acknowledges and agrees that the Company and/or its licensors own all Intellectual Property Rights in the Company's brands, trademarks and logos, the Cloud Based Technology, the Access and any Company Content. Except as expressly stated in these Terms of Use the Company does not grant the Customer any rights in respect of those rights.

6.2 Subject to clause 6.3, the Customer and/or its licensors shall, as between the parties, remain the owner of all Intellectual Property Rights in the Customer Data.

6.3 The Customer grants the Company, free of charge, a royalty-free, worldwide, non-exclusive licence to use the Customer Data as is necessary to enable the Company to:
(i) provide Access;
(ii) perform its obligations under these Terms of Use; and
(iii) improve its services and offerings including training its personnel during and after the Term and include any Confidential Information received by Company from Customer in the form of documents and data associated with the documents into training data ("**Training Data**") for inclusion in the training dataset of the Company's Cloud Based Technology. Training Data shall be still owned by the Customer. For the avoidance of doubt: (a) Training Data shall be considered to be Confidential Information of the Customer; (b) any derivations of the Training Data produced by the Company shall be owned exclusively by the Company.

The Customer warrants that it owns the Customer Data and/or is otherwise entitled to grant the foregoing licence. If these Terms of Use are terminated, the foregoing licence will automatically terminate in respect of any future Customer Data, but not in respect of any Customer Data already provided.

6.4 The Customer shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of the Customer Data.

7. Data Processing

7.1 For the purposes of this clause 7 and Data Processing Schedule, "**controller**", "**processor**", "**personal data**", "**process/processing**", **"sub-processor**" "**technical and organisational measures**" and "**supervisory authority/authority**" shall have the meaning as set out in the applicable Data Protection Laws or (where specifically defined therein);

7.2 Each party shall comply with its obligations under applicable Data Protection Laws and, to the extent applicable under the Data Protection Laws, obtain and maintain all appropriate registrations required in order to allow that party to perform its obligations under these Terms of Use.

Data processors

7.3 Where the Company is deemed to be acting as a processor for the Customer with respect to Personal Data shared in relation to these Terms of Use under applicable Data Protection Laws, the Data Processing Schedule shall apply to such processing.

Data controllers

7.4 Where a party is deemed to be acting as a controller with respect to personal data processed under or in relation to these Terms of Use, under applicable Data Protection Laws, this clause 7.4 shall apply, and each party shall, in its capacity as a controller:

(a) provide assistance to allow the other party to comply with any data subject requests (whether in relation to access to Customer personal data, rectification, restrictions on processing, erasure or portability) insofar as possible;

(b) provide assistance to allow the other party to comply with any other queries or complaints from a supervisory authority (as defined in Data Protection Laws) insofar as possible; promptly notify the other party of any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed pursuant to these Terms of Use ("Security Incident"); and

(c) provide reasonably necessary assistance to enable the other party to notify insofar as possible: (i) the relevant supervisory authority, promptly and in any event no later than 72 hours after relevant data controller becomes aware of a Security Incident; and (ii) the relevant data subjects without undue delay (where required) of a Security Incident.

7.5 If in the Company's reasonable opinion the relevant data protection provisions of these Terms of Use need to be amended in order to comply with the Company's obligations; or pursuant to any supervisory authority opinion or guidance, the Company shall be entitled to unilaterally amend this clause 7 and the Data Processing Schedule upon giving 30 days' notice to the Customer.

7.6 For clarity, this clause 7 and the DPA do not apply in respect of any Reseller Partner (as the relevant data protection provisions are set out separately in the Reseller Agreement).

8. Indemnities

8.1 The Customer hereby indemnifies the Company from and against any and all losses, damages, claims, costs and expenses (including reasonable external legal expenses) suffered or incurred by or awarded against the Company as a result of, or in connection with, any Customer Data or the Company's receipt, possession and/or use, in accordance with these Terms of Use, of any Customer Data.

8.2 The Company will indemnify the Customer from and against any and all losses, damages, claims, costs and expenses (including reasonable external legal expenses) suffered or incurred by or awarded against the Customer as a result of any claim against the Customer by a third party that the Customer's use of the Cloud Based Technology infringes the intellectual property rights of any person (save to the extent caused by the Customer Data).

9. Confidentiality

9.1 Subject to clauses 6.3 and 7, neither party shall without the consent of the other during the term of these Terms of Use (or for a period of 10 years following disclosure of the particular Confidential Information) disclose the other party's Confidential Information and only use such Confidential Information as strictly necessary for the performance of, or exercise of its rights under, these Terms of Use.

9.2 Subject to clauses 6.3 and 7, any party disclosing Confidential Information in accordance with the above clause shall procure that the person to whom such information is disclosed is made aware of the obligations of confidentiality under these Terms of Use and complies with those obligations as if it were a party to these Terms of Use.

9.3 The confidentiality restrictions do not apply to Confidential Information (but excluding Personal Data):

(a) which is in or comes into the public domain other than through breach of these Terms of Use;

(b) insofar as it comes lawfully into the possession of the recipient party from a third party;

(c) which the recipient party can prove was already known to it before its receipt from the providing party;

(d) to the extent that it is required to be disclosed by law or the requirements of any recognised stock exchange, or authority of competent jurisdiction to whose rules the party making the disclosure is subject, whether or not having the force of law.

9.4 Subject to clause 6.3, the Company acknowledges that the Customer Data is the Confidential Information of the Customer, and the Customer acknowledges that details of these Terms of Use, Access Fees and the Company Content, are the Confidential Information of the Company.

10. Liability

10.1 Nothing in these Terms of Use shall in any way exclude or limit either party's liability: (i) death or personal injury caused by either party's negligence or for fraudulent misrepresentation; (ii) for any other fraudulent act or omission; (iii) to pay sums properly due and owing to the other in the normal course of performance of these Terms of Use; or (iv) for any other liability which may not be excluded by law.

10.2 Subject to clause 10.1, neither party will be liable for any of the following losses or damage (whether or not such losses or damage were foreseen, direct, foreseeable, known or otherwise) howsoever arising:

(a) loss of revenue, sales, turnover, revenue or business, customers, contracts or opportunity, waste of management or other staff time, actual or anticipated profits, anticipated savings, business, opportunity, goodwill, reputation, hardware, software or data or damage to or corruption of data;

(b) any, indirect, special or consequential loss or damage howsoever caused whether or not such loss is covered in clause 10.2(a); or

(c) any losses arising as a result of any third party bringing a claim in respect of any of the types of loss in clause 10.2(a).

10.3 Subject to clause 10.1, the Company shall not be liable, whether in contract, tort (including negligence), breach of statutory duty, under any indemnity or otherwise, for any loss, damage, expense or liability incurred or sustained as a result of the use of the Cloud Based Technology and/or the Access except for their normal intended purpose, any modification to Access, the continued use of any out of date version of the API, or the processing of any Customer Data.

10.4 Subject to clauses 10.1, 10.2 and 10.3 the Company's total aggregate liability arising out of, or in connection with these Terms of Use for negligence or breach of contract or any other reason shall in no event exceed the Access Fees paid.

11. Term and Termination

11.1 Where the Company agrees to provide a Customer with Access directly (rather than via a Reseller), the parties shall specify in an Access Order

(a) the target date on which the Company shall begin to provide the Customer with Access (which may or may not be the same as the signature date of that Access Order) ("**Start Date**");

(b) the date on which the Company shall stop providing the Customer with Access ("**End Date**"); and

(c) whether there are any renewal rights.

11.2 These Terms of Use shall automatically renew at the end of the Term for a further 12 months (each period a "**Renewal**" or "**Renewal Term**"), and the same will apply on each anniversary of each Renewal, save where either party gives the other not less than 60 days' notice prior to the end of the Term or any Renewal.

11.3 Unless otherwise agreed, the "**Term**" commences on the earlier of the Free Trial commencement or the date the parties both sign the first Access Order and ends on the later of the end of the Free Trial Term or the End Date (as applicable).

11.4 The Company may without liability, terminate these Terms of Use, or alternatively, may suspend Access to and use of the Cloud Based Technology, by giving the Customer written notice if:

(a) any invoiced amount (not then-currently being disputed in good faith) is outstanding beyond the due date for payment;

(b) any provision of clause 5 or 6 is breached; and/or

(c) the Customer is in persistent or repeated breach of any of its obligations under these Terms of Use (whether or not it is the same obligation that is breached and whether or not such breaches are remedied),

and, in each case, the Customer has not remedied the issue in full to the Company's satisfaction within 10 days of the Company requiring it to do so.

11.5 Either party may terminate this Agreement immediately upon notice if the other party becomes Insolvent.

11.6 Termination of an individual Access Order shall not affect other Access Orders. Termination of these Terms of Use shall automatically terminate all Access Orders.

11.7 On termination of these Terms of Use for any reason:

(a) all licences granted under these Terms of Use shall immediately terminate;

(b) the Customer shall return and make no further use of, or access, any Cloud Based Technology, documentation and other items (and all copies of them) belonging to the Company (if any);

(c) all amounts payable to the Company by the Customer shall become immediately due and owing (and no refund of Access Fees paid in advance shall be due in respect of any unexpired portion of the then-current Term including any fee paid in respect of any Proof of Concept phase); and

(d) the accrued rights of the parties as at termination, or the continuation after termination of any provision expressly stated to survive or implicitly surviving termination, shall not be affected or prejudiced.

12. General

12.1 Neither party shall have any liability or be deemed to be in breach of these Terms of Use for any delays or failures in performance of this Agreement which result from circumstances beyond the reasonable control of that party including, without limitation, any of the following: power failure, act of God, governmental act, war, fire, flood, explosion or civil commotion. The party affected by such circumstances shall promptly notify the other party in writing when such circumstances cause a delay or failure in performance and when they cease to do so. If an event of force majeure occurs and lasts for more than 90 days either party may give written notice to the other to terminate these Terms of Use and neither party will have any liability to the other except that the Customer will remain liable for any unpaid Access Fees.

12.2 The failure or delay by either party to enforce the terms of these Terms of Use or to exercise any remedy or right shall not be treated as a waiver of any breach or right to enforcement or exercise. If any part of these Terms of Use is ruled illegal, void or unenforceable then that part shall be deemed not to be a part of this Agreement and the enforceability of the remainder of these Terms of Use shall not be affected.

12.3 The Customer shall not, without the prior written consent of the Company, assign any of its rights or obligations under these Terms of Use. These Terms of Use may not be varied except in writing signed by the authorised representatives of all the parties to these Terms of Use.

12.4 Nothing in these Terms of Use shall be deemed to constitute a partnership or joint venture or contract of employment between the parties nor constitute either party the agent of the other. These Terms of Use does not confer any rights on any third party pursuant to the Contracts (Rights of Third Parties) Act 1999.

12.5 Neither party shall make or issue any announcement or public circular relating to the subject matter of these Terms of Use without the prior written approval of the other. The Company may use the name of Customer as a factual reference to the fact that the Customer is or was a customer, on its website and in pitch materials, without the prior written consent of Customer.

12.6 Each party shall at all times ensure that it complies with the terms of the Bribery Act 2010 and that it does not commit (or procure the commission of) any breach of that Act. These Terms of Use, and any documents explicitly referred to in it, constitute the whole agreement between the parties and supersede any previous arrangement, understanding or agreement between them relating to the subject matter they cover.

12.7 Each of the parties acknowledges and agrees that in entering into these Terms of Use it does not rely on any undertaking, promise, assurance, statement, representation, warranty or understanding (whether in writing or not) of any person (whether party to these Terms of Use or not) relating to the subject matter of these Terms of Use, other than as expressly set out in this Agreement.

12.8 In the event of any inconsistencies between the terms set out in the DPA, the Access Order and these Terms of Use, the terms shall be construed in the same order.

12.9 These Terms of Use are governed by English law. Both parties submit to the exclusive jurisdiction of the English courts in relation to any dispute arising out of or in connection with these Terms of Use or its subject matter, but the Company is also entitled to apply to any court worldwide for injunctive or other remedies in order to protect or enforce its Intellectual Property Rights.

13. **Definitions and interpretation**

"Access" is defined in clause 2.1;

“Access Fees” means the access fees for Access as specified in the Access Order being payable either directly by the Customer (in the event that the Customer contracts directly with the Company) or the Reseller Partner (in the event that the Customer procures Access from a Reseller);

“Access Methods” means any and all of: URL, user id, API key and similar that enable the Customer to work with the Cloud Based Technology;

“Access Order” means as applicable: (a) the Customer's written instruction (including in electronic form) directly from the Customer to the Company to provide Access; or (b) the written instructions (including in electronic form) from the Reseller Partner to the Company to provide Access to the Reseller Partner and/or any downstream end users (including the Customer), in both cases incorporating, and subject to, these terms of use;

"Affiliate" means, with respect to either party, any corporate entity that is directly or indirectly controlled by, or is under the common control of such party (but only for so long as such control exists), where "control" means holding, directly or indirectly, a majority of the voting rights in it, or the power to direct or cause the direction of its management, policies or operations (whether through holding of voting rights, by contract or otherwise);

"API" means the Company's API to allow Access;

"Cloud Based Technology" means the Company's cloud based technology for data extraction from documents, the cloud based user interface for verification and correction of the extracted data, the extension environment and the reporting database;

"Company" means Rossum Ltd, 71 – 75 Shelton Street, Covent Garden, WC2H 9JQ London, United Kingdom and its Affiliates;

"Company Content" means all data, information and material owned by or licensed to the Company and comprised within the Cloud Based Technology and/or Access, but excluding Customer Data;

"Confidential Information" means all information (whether written, oral or in some other form) disclosed to or obtained by one party (whether directly or indirectly) from the other (whether before or after the signing of these Terms of Use), including all information relating to that other's business, operations, systems, processes, products, trade secrets, know how, contracts, finances, plans, strategies or current, former or prospective clients, customers, partners or suppliers (together with copies made of any of the foregoing) and which information is marked as being confidential or might reasonably be assumed to be confidential and which includes Personal Data unless otherwise specified or the context so requires;

“Customer” means the end user customer who is receiving Access either: (a) directly from the Company under an Access Order, and whose details are set out in that Access Order; or (b) by purchasing via a Reseller Partner, and any of their Affiliates;

“Customer Data” means all information, data or other materials inputted into the Cloud Based Technology by the Customer or otherwise on its behalf, including information automatically extracted from the Customer documents and information manually corrected on the Cloud Based Technology by or on behalf of a Customer;

"Data Protection Laws" means all privacy laws applicable to any personal data processed under or in connection with these Terms of Use, including, without limitation, the General Data Protection Regulation 2016/679 (the "GDPR")), the Privacy and Electronic Communications Directive 2002/58/EC (as the same may be superseded by the Regulation on Privacy and Electronic Communications ("ePrivacy Regulation")) and all national legislation implementing or supplementing the foregoing and all associated codes of practice and other guidance issued by any applicable data protection authority, all as amended, re-enacted and/or replaced and in force from time to time;

"Data Processing Schedule" or "DPA" means the Data Processing Schedule attached to these Terms of Use;

“Free Trial” or "**Free Trial Term**" have the meanings set out in clause 3.1;

“Insolvent” means, in relation to a party, where that party becomes insolvent, makes composition with its creditors, has a receiver or administrator of its undertaking or the whole or a substantial part of its assets appointed, or an order is made, or an effective resolution is passed, for its administration, receivership, liquidation, winding-up or other similar process, or has any distress, execution or other process levied or enforced against the whole or a substantial part of its assets (which is not discharged, paid out, withdrawn or removed within 28 days), or is subject to any proceedings which are equivalent or substantially similar to any of the foregoing under any applicable jurisdiction, or ceases to trade or threatens to do so;

“Intellectual Property Rights” means patents, patentable rights, copyright, design rights, utility models, trade marks (whether or not any of the above are registered), trade names, rights in domain names, rights in inventions, rights in data, database rights, rights in know-how and confidential information, and all other intellectual and industrial property and similar or analogous rights existing under the laws of any country and all pending applications for and right to apply for or register the same (present, future and contingent, and including all renewals, extensions, revivals and all accrued rights of action);

"Personal Data" means all data which is defined as 'personal data' under Data Protection Laws and which is provided by the Customer to the Company (directly or indirectly), and accessed, stored or otherwise processed by the Company as a data processor as part of its provision of the Access to Customer and to which Data Protection Laws apply from time to time;

"Proof of Concept" or "Proof of Concept Term" means the proof of concept phase described in an Access Order and the related duration set out in that Access Order;

"Reseller Partner" means an authorised partner reseller of Access through which a Customer may procure Access. For clarity, each Reseller Partner must enter into a "**Reseller Agreement**" as between the Company and Reseller;

"Term" has the meaning set out in clause 11.3;

"Terms of Use" means these terms of use together with all the recitals, clauses, schedules, annexes and all other documents referred to herein and, in the event that the Customer procures Access directly from the Company, the Access Order; and

"URL" means the Company's web URL through which the Customer will access the Cloud Based Technology.

In this Agreement: (i) references to persons include all forms of legal entity including an individual, company, body corporate, unincorporated association and partnership; (ii) the word "including" is to be construed as being by way of illustration only and is not to be construed so as to limit the generality of any preceding words; (iii) the words "other" and "otherwise" are not to be construed as being limited by any words preceding them; (vi) headings are used for convenience only and do not affect its interpretation; (v) singular includes the plural, and vice versa; and (vi) reference to a "party" or "parties" means the parties to these Terms of Use, being the Company and the Customer or Reseller Partner, as applicable.

DATA PROCESSING SCHEDULE

1. Definitions

1.1 In addition to the definitions set out in clauses 7 and 13 of the Terms of Use, the following terms have the corresponding meanings:

"Adequate Country" means a country or territory outside the EEA recognised as providing adequate protection for Personal Data transfers under an adequacy decision made from time to time by the European Commission under the GDPR;

"Company Group" means the Company and any of its Affiliates;

"Customer Group" means the Customer and any of its Affiliates established and/or doing business in the EEA, or the United Kingdom;

"Data Subject Request" means a request from or on behalf of a data subject relating to access to, or rectification, erasure or data portability in respect of that person's Personal Data or an objection from or on behalf of a data subject to the processing of its Personal Data;

"EEA" means European Economic Area and Switzerland;

"Model Clauses" means the model clauses for the transfer of personal data to processors established in third countries approved by the European Commission, the approved version of which is set out in the European Commission's Decision 2010/87/EU of 5 February 2010 and at http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087 and which form a part of this DPA; and

"Privacy Shield Principles" means the Swiss-U.S. and EU-U.S. Privacy Shield principles (as may be amended, superseded or replaced) and available from the US Department of Commerce at https://www.privacyshield.gov/EU-US-Framework.

2. Status of the Parties

2.1 The type of Personal Data processed pursuant to this DPA and the subject matter, duration, nature and purpose of the processing, and the categories of data subjects, are as described below, and may be updated by Customer's further written instructions:

(a) The subject matter of the processing comprises: the processing of Personal Data under or in relation to these Terms of Use;

(b) The nature of the processing comprises: (i) Business activities of the Company in relation to the Customer (such as marketing, sales, solution consulting and customer success).
(ii) Storage, data capture (as configured) and provision of product features (such as user management and reporting) to the Customer in relation to any Personal Data that may be contained on the processed documents. ;

(c) The purpose(s) of the processing is/ are: Processing for the provision of the Access, administration, support, and delivery of product services to all customers. ;

(d) The personal data comprises: For business contacts and user accounts, up to: name, address (postal), address (email), phone number, mobile phone number, job title, position, and other information relevant to the interaction with the data subject or the Customer or other undertaking for which they work. For documents and captured data, depending on Customer's configuration of the system and data submitted by the Customer. ;

(e) The categories of data subjects and types of personal data included in the processing are: Customers and prospective customers, employees and temporary staff, prospective employees and temporary staff, participants in market research surveys, user account holders, data subjects who are identified in or identifiable via documents as submitted by the Customer.;

(f) The duration of the processing will be: until the date upon which processing is no longer necessary for the purposes of either party performing its obligations under the Terms (to the extent applicable); and

(g) Approved international transfers are: those set out in the DATA SUBPROCESSOR SCHEDULE.

2.2 Each party warrants in relation to Personal Data that it will comply (and will procure that any of its personnel comply and use commercially reasonable efforts to procure that its sub-processors comply), with the Data Protection Laws.

2.3 As between the parties, the Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Customer acquired Personal Data.

2.4 In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties hereby acknowledge and agree that the Customer is the data controller and the Company is the data processor and accordingly the Company agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPA.

2.5 Each party shall appoint an individual within its organisation authorised to respond from time to time to enquiries regarding the Personal Data and each party shall deal with such enquiries promptly.

3. The Company obligations

With respect to all Personal Data, the Company shall:

3.1 process Personal Data (i) in order to provide the Access, and/or (ii) as set out in: (A) the Terms of Use, (B) this DPA, and (C) Customer's written instructions;

3.2 in the unlikely event that applicable law requires the Company to process Personal Data other than pursuant to the Customer's instruction, the Company will notify the Customer (unless prohibited from doing so by applicable law);

3.3 as soon as reasonably practicable upon becoming aware, inform the Customer if, in the Company's opinion, any instructions provided by the Customer under paragraph 3.1 of this Schedule infringe the GDPR;

3.4 implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data. Such measures include, without limitation, the security measures set out in the SECURITY MEASURES SCHEDULE;

3.5 take reasonable steps to ensure that only authorised personnel have access to such Personal Data and that any persons whom it authorizes to have access to the Personal Data are under obligations of confidentiality;

3.6 as soon as reasonably practicable upon becoming aware, notify the Customer of any actual incident of unauthorised or accidental disclosure of or access to any Personal Data by any of its staff, sub-processors, or any other identified or unidentified third party (a "Security Breach");

3.7 promptly provide the Customer with reasonable cooperation and assistance in respect of a Security Breach and all reasonable information in the Company's possession concerning the Security Breach insofar as it affects the Customer and/or any member of a Customer Group;

3.8 not make any public announcement about a Security Breach (a "Breach Notice") without the prior written consent from the Customer unless required to make a disclosure or announcement by applicable law;

3.9 promptly notify the Customer if it receives a Data Subject Request. To the extent the Customer does not have the ability to address a Data Subject Request, the Company shall upon the Customer's request provide reasonable assistance to facilitate a Data Subject Request to the extent the Company is able to consistent with applicable law, provided the Customer shall pay the Company's charges for providing such assistance;

3.10 other than to the extent required to comply with applicable law, the Company will delete (including by putting beyond practicable use) or return all Personal Data held in Cloud Based Technology databases and for which the Company is the Processor and that is processed pursuant to this DPA, and the parties shall agree the timing, scope and costs of such deletion or return at the time of termination or expiry of the Terms or expiry of the Access; and

3.11 provide such assistance as the Customer reasonably requests (taking into account the nature of processing and the information available to the Company) to the Customer in relation to the Customer's obligations under Data Protection Laws with respect to: (i) data protection impact assessments (as such term is defined in the GDPR); (ii) notifications to the supervisory authority under Data Protection Laws and/or communications to data subjects by the Customer in response to any Security Breach; and (iii) Customer's compliance with its obligations under the GDPR with respect to the security of processing,

provided the Customer shall pay the Company's charges for providing the assistance in this paragraph 3.11.

4. Sub-processing

4.1 The Customer grants a general authorisation (a) to the Company to appoint other members of the Company Group as sub-processors and (b) to the Company and other members of the Company Group to appoint third parties as may be required as sub-processors to support the provision of the Access.

4.2 The Company will maintain a list of sub-processors that it engages to process Personal Data as the DATA SUBPROCESSOR SCHEDULE, which it may update from time to time, and will provide such updated list upon written request by the Customer , Company will notify the Customer by adding the names of new and replacement sub-processors to the list prior to them starting sub-processing of Personal Data.

(a) If the Customer has a reasonable objection to any new or replacement sub-processor, it shall notify the Company of such objections in writing within ten (10) days of the notification.

(b) If the Company and the Customer are unable to reach agreement in respect of Company's use of the new or replacement sub-processors within thirty (30) days from the Customer's notification of objections, the Customer may within ten (10) days of the end of the thirty (30) day period terminate the Terms by providing written notice to the Company having effect thirty (30) days after receipt by the Company.

(c) If the Customer does not provide a timely objection to any new or replacement sub-processor in accordance with this paragraph 4.2, the Customer will be deemed to have consented to the sub-processor and waived its right to object.

(d) The Company will refund to the Customer any prepaid fees covering the remainder of the term of the Terms of Use following the date of termination.

4.3 The Company will ensure that any sub-processor it engages to provide an aspect of the Access on its behalf in connection with this DPA does so only on the basis of a written contract which imposes on such sub-processor terms substantially no less protective of Personal Data than those imposed on the Company in this DPA (the "Relevant Terms"). The Company shall procure the performance by such sub-processor of the Relevant Terms and shall be liable to the Customer for any breach by such person of any of the Relevant Terms.

5. Audit and records

5.1 The Customer may reasonably request such information (in the Company's possession or control) as may be required to demonstrate Company's compliance with the obligations of processors under Data Protection Laws in relation to its processing of Personal Data, provided the Customer shall pay Company's reasonable charges for providing the assistance in this paragraph 5.1. Company shall endeavour to provide such information within a reasonable period of time.

5.2 The parties acknowledge that the Customer has certain audit rights under Data Protection Law. The Company shall fulfil the the Customer's right of audit under Data Protection Laws and Company shall endeavour to provide such information within a reasonable period of time.

6. Data transfers

Transfer mechanisms

6.1 The Company processes Personal Data within the EEA and may, subject to paragraph 6.2 of this DPA, process Personal Data outside the EEA.

6.2 To the extent any processing of Personal Data by the Company takes place in any country outside the EEA (except if in an Adequate Country), the parties agree that the Model Clauses will apply in respect of that processing and that:

(a) the Company is the 'data importer' and will comply with the obligations of the 'data importer' in the Model Clauses accordingly; and

(b) the Customer is the 'data exporter' and will comply with the obligations of the 'data exporter' accordingly.

6.3 The following terms shall apply to the Model Clauses:

(a) the Customer may exercise its right of audit under clause 5(f) of the Model Clauses as set out in, and subject to, the requirements of paragraph 5 of this DPA; and

(b) the Company may appoint sub-processors as set out, and subject to, the requirements of paragraphs 4 and 6.5 of this DPA.

Sub-processors – transfer mechanisms

6.4 The Customer acknowledges and accepts that the provision of the Access under the Terms may require the processing of Personal Data by sub-processors in countries outside the EEA from time to time.

6.5 If, in the performance of this DPA and/or the Terms, the Company transfers any Personal Data to a sub-processor (which shall include without limitation any Affiliates of the Company) and without prejudice to paragraph 4, where such sub-processor will process Personal Data outside the EEA (except if in an Adequate Country), the Company shall, in advance of any such transfer, take steps to put in place a legal mechanism to achieve adequacy in respect of that processing, such as:

(a) the requirement for the Company to execute or procure that the sub-processor execute Model Clauses;

(b) the requirement for the sub-processor to be certified under the EU-U.S. Privacy Shield Framework; or

(c) the existence of any other specifically approved safeguard for data transfers (as recognized under Data Protection Laws) and/or a European Commission finding of adequacy.

6.6 Upon reasonable request by Customer, the Company shall make available to the Customer evidence of such legal mechanisms which are in place with relevant sub-processors.

ACCEPTABLE USE SCHEDULE

Users of the Rossum application, platform and APIs shall, unless receiving a prior express approval by the Company, not disrupt the service by:

1. Overloading the platform. The Customer shall abide to these limits, in aggregate over all concurrent sessions pertaining their Access Order (organization account).
    a. No more than 600 API requests per minute.
    b. No more than 600 application page loads per minute.
    c. No more than 600 application logins or API logins per hour.
    d. No more than 600 document uploads per hour, in total size of no more than 6 GiB of data.
    e. No more than 600 queue exports per hour.
    f. Other activity that could reasonably be understood as a Denial-of-Service attack.
2. Attacking the security of the platform, by manually or automatically attempting to breach any security controls, including brute forcing passwords or secret tokens, attempting to exploit software vulnerabilities, or systematically attempting to access API objects not associated with their Access Order (organization account).

SECURITY MEASURES SCHEDULE

Technical and organizational measures employed by Rossum include:

A. Access control

Denying unauthorized persons access to the processing equipment used for data processing:

(a) Access to the business / IT rooms:

1. The business premises are always locked outside of business hours.
2. The business premises are either automatically locked during business hours and access secured via a chip-based access control system or staffed reception, or employees are obliged to lock doors when leaving.
3. There is an elevator control system that prevents unauthorized persons from gaining access to the anterooms outside of business hours.
4. The doors to the stairwell are also locked at these times.
5. The building of the business premises is locked outside of business hours or behind a reception with all visitors reporting.
6. The on-premises server rooms are secured by an additional lock system with only qualified personnel having access.
7. The cleaning staff is carefully selected and the cleaning staff are known in advance.

(b) Access to data processing systems:

1. The company office network is secured by a firewall.
2. The production network is secured by a firewall.
3. All workstations on which sensitive data are processed are encrypted (FileVault, Bitlocker, encrypted containers).
4. Employees are required to lock their computers when they are away and to use secure passwords / passphrases.
5. On-premise server systems are either encrypted or secured by physical access protection in such a way that no access to the hardware is possible.
6. Data are processed on full scale only on production systems hosted in cloud, with servers located in ISO-27001 certified, SOC-2 audited physical data centers.
7. Access to systems is generally only possible with user-specific authentication (user name / password / RSA key) and on a need-to basis.
8. All production systems are kept up to date regarding any known vulnerabilities at all times, only supported systems are used.

B. Data carrier control

Prevention of unauthorized reading, copying, changing or deleting of data carriers:

1. All workstations on which data is processed are encrypted.
2. Server systems are either encrypted or secured by physical access protection in such a way that no access to the hardware is possible.
3. Before transferring (selling) or disposing of data carriers, they will be securely deleted.
4. Defective data carriers or data carriers that can no longer be deleted for other reasons are collected by the IT department and stored securely until they are handed over to a data shredder certified according to ISO-IEC 21964.
5. All production infrastructure is reviewed prior to any modification and described as version controlled code.
6. All production data is stored redundantly and backed up.
7. There are internal schedules, guidelines, contractual obligations for employees (guidelines for information security / data protection, confidentiality agreements, obligation to maintain data secrecy).

C. Storage control

Prevention of unauthorized entry of personal data as well as unauthorized access, modification and deletion of stored sensitive data:

1. Systems must be locked in accordance with internal guidelines when they are away.
2. All workstations on which personal data are processed are encrypted.
3. Server systems are either encrypted or secured by physical access protection in such a way that no access to the hardware is possible.
4. Users have to authenticate themselves on all systems with their personal access data.
5. Depending on the system, there are individual authorization concepts.
6. Test and production systems are strictly separated.
7. There are internal schedules, guidelines, contractual obligations for employees (guidelines for information security / data protection, confidentiality agreements, obligation to maintain data secrecy).
8. Any third-party data processors are subject to management approval, need to hold security certifications appropriate to scale of the data processing performed, and listed in the **DATA SUBPROCESSOR SCHEDULE** below. Data processing contacts are properly concluded as appropriate.
9. Security policy requires a regular penetration test performed (at least annually).

D. User control

Prevention of the use of automated processing systems with the help of devices for data transmission by unauthorized persons:

1. Only authorized persons have access to data processing systems; per server / service / software there are different authorization concepts with different authorization levels and rights per user.
2. Users have to authenticate themselves on all systems with their personal access data.
3. If personal data is transmitted via the Internet, this is done exclusively via encrypted transmission channels.
4. Centralized audit log of all software operations performed in the production system is maintained.
5. Test and production systems are strictly separated.
6. There are internal schedules, guidelines, contractual obligations for employees (guidelines on information security / data protection, confidentiality agreements, obligation to maintain data confidentiality).
7. New employees are vetted via reference checks and other appropriate methods.
8. An offboarding process policy ensures that on the day of leaving, all user accounts of an employee are blocked.

E. Access level control

Ensuring that those authorized to use an automated processing system only have access to the data covered by their access authorization:

1. Access to systems is only possible with user-specific authentication (including MFA where applicable).
2. Each employee has different authorization levels on individual systems, on a need-to basis.
3. An onboarding policy ensures that only authorized persons have access to data processing systems; per server / service / software there are different authorization concepts with different authorization levels and rights per user.
4. Internal security policies include regular security reviews from process and access perspective (at least quarterly).

F. Transmission control

Ensuring that it can be checked and ascertained to which locations data has been or can be transmitted or made available with the aid of data transmission facilities:

1. Every access as well as the transmission of data are logged.
2. There are strictly defined transmission channels and internal processes for the transmission of data provided by the customer.
3. Third-party systems processing data are vetted based on string criteria (in particular standing certifications) and periodically reviewed
4. All services available via the Internet can only be accessed via encrypted connections.

5. Each system has its individual log files, logs are centrally aggregated.

G. Entry control

Ensuring that it can be subsequently checked and ascertained which data was entered or changed in automated processing systems at what time and by whom:

1. Each system has its individual log files, logs are centrally aggregated.
2. The acquisition and modification of all data records is carried out with time stamp and user name logged; there is a detailed change log for personal data.

H. Transport control

Ensuring that the confidentiality and integrity of the data are protected when transmitting data and when transporting data carriers:

1. There are strictly defined transmission channels and internal processes for the transmission of data provided by the customer.
2. All workstations / notebooks on which personal data are processed / transported are encrypted.
3. All services available via the Internet can only be accessed via encrypted connections.
4. Data media delivered by customers are safely stored, deleted or returned to the customer by the IT department.

I. Recoverability

Ensuring that systems used can be restored in the event of a fault:

1. Multi-level backups with individually adapted backup concepts exist for all systems: Data can be redacted from the primary systems but not necessarily from all backup levels.
2. Hardware and software are designed redundantly; Systems are used which guarantee the redundancy of the contents of data carriers or entire machines.
3. The internal network infrastructure has a redundant structure.
4. A written security incident response policy ensures appropriate handling of a security breach.

J. Reliability

Ensuring that all system functions are available and any malfunctions that occur are reported (reliability):

1. All systems are monitored, vitals aggregated, alerts triggered based on error conditions.
2. Temperature, water and fire detectors are installed in the server rooms. Production systems are resilient to power outages.
3. Employees are required to report any system malfunctions to the IT department immediately.
4. IT security team periodically reviews the complete infrastructure and enacted policies, assesses threats and rectifies any action points identified.

K. Data integrity

Ensuring that stored data cannot be damaged by system malfunctions:

1. See also point J. Reliability.
2. All production data is stored redundantly and backed up.
3. Managed cloud storage layers automatically detect data corruption.
4. Server systems are individually hardened.
5. All code changes go through a strict code review process and multi-stage code integration (continuous integration) and testing before a production release.
6. User rights are granted as restrictively as possible.

L. Order control

Ensuring that personal data processed in the order can only be processed in accordance with the instructions of the person responsible:

1. Instructional contracts with our customers explicitly specify instructions recipients and authorized representatives.
2. Employees are trained in data protection and are required to follow internal information security policy.
3. All employees are obliged to maintain confidentiality in accordance with the employment contract and also via "obligation to maintain data confidentiality" in accordance with the GDPR.
4. Automatic processing of personal data acquired externally is subject to automatic policies excluding processing of data without consent, policies are applied automatically to delete personal data when the reason for its processing ceases.
5. Access to customer data databases are only given to employees requiring it.
6. Compliance with internal processes / guidelines is continuously monitored, any issues are escalated to the company management.

M. Separability

Ensuring that data collected for different purposes can be processed separately:

1. Internally used personal data systems offer the possibility to process people separately according to contact status.
2. Test and production systems are strictly separated.

DATA SUBPROCESSOR SCHEDULE

Third-party vendors processing or potentially regularly processing or having access to Confidential Information and/or Personal Data:

Subprocessor	**Legal Jurisdiction**	**Personal Data Location**
Amazon Web Services EMEA SARL	Luxembourg	Ireland, EU (unless agreed otherwise)
Google LLC	U.S.	EEA and non-EEA (Privacy Shield)
Microsoft Corporation	U.S	EEA and non-EEA (Privacy Shield)
LogMeIn, Inc.	U.S.	*no personal data storage*
Slack Technologies, Inc.	U.S.	EEA and non-EEA (Privacy Shield)

Third-party vendors that may exceptionally process Confidential Information and/or Personal Data:

Third - party vendor	**Legal Jurisdiction**	**Personal Data Location**
HubSpot, Inc.	U.S.	Ireland and U.S. (Privacy Shield)
Freshworks, Inc.	U.S.	EEA and non-EEA (Privacy Shield)
Smartsupp.com, s.r.o.	Czech Republic	EU
Rollbar, Inc.	U.S.	EEA and non-EEA (Privacy Shield)
Zoom Video Communications, Inc.	U.S.	EEA and non-EEA (Privacy Shield)