Data Processing Addendum

Notion has updated its Data Processing Addendum effective February 22, 2023. For existing Users, these updates will apply beginning on March 4, 2023. For new Users, these updates apply immediately. To view the previous version of Notion's Data Processing Addendum, click the link below 👇

🌐 Data Processing Addendum (Deprecated February 22, 2023)

This Data Processing Addendum (“**DPA**”) forms part of the Master Subscription Agreement (the “**Agreement**”) between Customer and Notion Labs, Inc. (”**Notion**”).

1. Subject Matter and Duration

1.1 Subject Matter. This DPA is intended to govern Customer's provision and Notion's Processing of Customer Personal Data pursuant to the Agreement. All capitalized terms that are not expressly defined in this DPA will have the meanings given to them in the Agreement. If and to the extent language in this DPA or any of its attachments conflicts with the Agreement, this DPA shall control.

1.2 Duration and Survival. This DPA will become binding upon the effective date of the Agreement and shall survive until expiration or termination of the Agreement or the return or deletion of Customer Personal Data in accordance with Section 8.1, whichever later.

2. Definitions

For the purposes of this DPA, the following terms and those defined within the body of this DPA apply.

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. and any associated regulations and amendments, including the California Privacy Rights Act amendments.

"**Controller**" means the person who, alone or jointly with others, determines the purposes and means of the Processing of personal data; for purposes of this DPA, the term "Controller" shall also include "business" as such term is defined under the CCPA.

"**Customer Personal Data**" means Customer Data that is "personal data" or "personal information" under applicable Data Protection Law.

"**Data Protection Law(s)**" means all worldwide data protection and privacy laws and regulations applicable to Customer Personal Data, including, where applicable, EU/UK Data Protection Law and the CCPA.

"**EEA**" means the European Economic Area.

"**EU/UK 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) the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (collectively, the "UK GDPR"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time;

“**Notion Security Standards**” means Notion’s security standards, as updated from time to time, available at: https://www.notion.so/help/security-and-privacy.

“**Process**” or “**Processing**” means any operation or set of operations which is performed on Customer Personal Data or sets of Customer Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

“**Processor**” means the person who, alone or jointly with others, Processes personal data on behalf of the Controller; for purposes of this DPA, the term "Processor" shall also include "service provider" as such term is defined under the CCPA.

"**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; and (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, in case whether such transfer is direct or via onward transfer.

"**SCCs**" means: (i) where the EU GDPR applies, the 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**"); and (ii) where the UK GDPR applies, standard data protection clauses for processors adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR ("**UK SCCs**").

“**Security Incident(s)**” means any unauthorized or unlawful breach of security leading to, or reasonably believed to have led to, the accidental or unlawful destruction loss, alteration, unauthorized disclosure or access to any Customer Data processed under or in connection with the Agreement, including but not limited to Customer Personal Data.

“**Subprocessor(s)**” means a third party engaged by Notion to Process Customer Personal Data under the Agreement.

3. Data Use and Processing

3.1 Data Processing Relationship. Customer is either the Controller of Customer Personal Data or else Processes Customer Personal Data as a Processor on behalf of a third-party Controller (such as an end customer to Customer). In either case, the parties acknowledge and agree that Notion has been appointed by the Customer to Process the Customer Personal Data as a Processor (or sub-Processor, as applicable) on behalf of the Customer. If Customer is a Processor on behalf of a third-party Controller, Customer will ensure that any Processing instructions it provides to Notion pursuant to this DPA shall be consistent with the instructions the Controller has issued to Customer.

3.2 Documented Instructions. Notion shall Process Customer Personal Data solely: (1) to fulfill its obligations to Customer under the Agreement, including this DPA; (2) on Customer's behalf; and (3) in compliance with Data Protection Laws. Notion shall Process Customer Personal Data strictly for the business purpose(s) agreed between the parties and as provided under the Agreement, this DPA, and any instructions expressly agreed upon by the parties in writing (together, the "**Business Purpose(s)**"). Customer will not instruct Notion to Process Customer Personal Data in violation of applicable law (including Data Protection Law(s)). Notion has no obligation to monitor the compliance of Customer's use of the Services with applicable law (including Data Protection Law(s)) and Notion will have no liability for any harm or damages resulting from Notion's compliance with unlawful Instructions received from Customer. However, Notion will, unless legally prohibited from doing so, (i) inform Customer in writing if it reasonably believes that there is a conflict between Customer's instructions and applicable law (including Data Protection Law(s)) or otherwise seek to Process Customer Personal Data in a manner that is inconsistent with Customer's instructions, and (ii) in either such event, cease all Processing of the affected Customer Personal Data (other than merely storing and maintaining the security of the affected Customer Personal Data) until such time as Customer issues new instructions with which Notion is able to comply. If this provision is invoked, Notion will not be liable to Customer under the Agreement for failure to perform the Services until such time as the parties agree on new instructions. Customer retains the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data, including any use of Customer Personal Data not authorized in this DPA.

3.3 Service provider certification. Notion shall not: (a) “sell” Customer Personal Data (as such term in quotation marks is defined in the CCPA), (b) “share” or Process Customer Personal Data for purposes of “cross-context behavioral advertising” or “targeted advertising” (as such terms in quotation marks are defined in the CCPA); (c) retain, use, or disclose Customer Personal Data for any purpose other than for the Business Purpose(s), including to retain, use, or disclose the Customer Personal Data for a commercial purpose other than performing its Services under the Agreement; (d) retain, use, or disclose the Customer Personal Data outside of the direct business relationship between Customer and Notion. Notion (i) will not attempt to re-identify any pseudonymized, anonymized, aggregate, or de-identified Customer Personal Data without Customer's express written permission; and (iii) will comply with any applicable restrictions under Data Protection Laws on combining the Customer Personal Data with personal data that Notion receives from, or on behalf of, another person or persons. Notion certifies that it understands the restrictions set out in this Section 3.3 and will comply with them.

3.4 Authorization to Use Subprocessors. Customer hereby authorizes Notion to engage affiliates and other Subprocessors to Process Customer Personal Data in accordance with the provisions within this DPA and Data Protection Laws. A current list of Notion’s Subprocessors can be found **here** ("Subprocessor List"). Customer acknowledges and agrees that Notion’s use of such Subprocessors satisfies the requirements of this DPA.

3.5 Notion and Subprocessor Compliance. Notion agrees to (i) enter into a written agreement with Subprocessors regarding such Subprocessors’ Processing of Customer Personal Data that imposes on such Subprocessors data protection requirements for Customer Personal Data that are consistent with this DPA; and (ii) remain responsible to Customer for Notion’s Subprocessors’ failure to perform their obligations with respect to the Processing of Customer Personal Data.

3.6 Notice of and Right to Object to New Subprocessors. Notion shall maintain an up-to-date list of its Subprocessors in its Subprocessor List. Customer should refer to the Notion Subprocessor List regularly. Customer may also sign up to receive notification of new Subprocessors by emailing team@makenotion.com with the subject “Subscribe to New Subprocessors.” Once Customer has signed up to receive new Subprocessor notifications, Notion will then provide Customer with notice of any new Subprocessor before authorizing such new Subprocessor to Process Customer Personal Data and allow Customer ten (10) days to submit a legitimate, good-faith objection to such new Subprocessor(s) from Customer’s receipt of Notion’s notice. In the objection, Customer shall explain its reasonable grounds for such objection. In the event of such objection, the parties will work together in good faith to resolve the grounds for the objection. If the parties are unable to resolve the objection within a reasonable time period, which shall not exceed thirty (30) days, either party may terminate the Agreement by providing written notice to the other party. Notion may replace a Subprocessor if the need for the change is urgent and necessary to provide the Services. In such instance, Notion shall notify Customer of the replacement as soon as reasonably practicable, and Customer shall retain the right to object to the replacement Subprocessor.

3.7 Confidentiality. Notion will ensure that any person whom Notion authorizes to Process Customer Personal Data on its behalf is subject to confidentiality obligations in respect of that Customer Personal Data.

3.8 Customer Personal Data Inquiries and Requests. To the extent Customer, in Customer’s use of the Services, does not have the ability to address a request from a data subject exercising their rights under applicable Data Protection Laws (e.g., access, deletion, etc.), Notion shall, upon Customer’s request, use commercially reasonable efforts to assist Customer in responding to such data subject request. If a request relating to Customer Personal Data is sent directly to Notion, Notion shall use commercially reasonable efforts to promptly notify Customer within five (5) business days of receiving such request and shall not respond to the request unless Customer has authorized Notion to do so. To the extent legally permitted, Customer shall be responsible for any non-negligible costs arising from Notion’s provision of assistance under this Section. Customer acknowledges that Notion is reliant on Customer for direction as to the extent to which Notion is entitled to Process Customer Personal Data on behalf of Customer in performance of the Services. Consequently, Notion will not be liable under the Agreement for any claim brought by a data subject arising from any action or omission by Notion, to the extent that such action or omission resulted from Customer’s instructions or from Customer’s failure to comply with its obligations under applicable law.

3.9 Data Protection Impact Assessment and Prior Consultation. Where and to the extent required by Data Protection Law(s), Notion agrees to provide Customer reasonable assistance to and cooperation for Customer’s performance of a data protection impact assessment of Processing or proposed Processing of Personal Data, when required by applicable Data Protection Laws, and at Customer’s reasonable expense.

3.10 Limitation on Disclosure of Customer Personal Data. To the extent legally permitted in each case, Notion shall: (i) promptly notify Customer in writing upon receipt of an order, demand, subpoena, warrant, legal demand or other document purporting to request, demand or compel the production of Customer Personal Data to any non-data-subject third party, including, but not limited to, regulatory authorities and the United States government for surveillance and/or other purposes; and (ii) not disclose Customer Personal Data to the third party without providing Customer at least forty-eight (48) hours′ notice, so that Customer may, at its own expense, exercise such rights as it may have under applicable laws to prevent, challenge or limit such disclosure to the extent permitted by applicable laws. If Notion is prohibited by applicable Data Protection Laws from disclosing the details of a government request to Customer, Notion shall inform Customer that it can no longer comply with Customer′s instructions under this DPA without providing more details and await Customer′s further instructions. Notion shall use all reasonable and available legal mechanisms to challenge any demands for data access through national security process that it receives, as well as any non-disclosure provisions attached thereto.

4. Cross-Border Transfers of Customer Personal Data

4.1 Cross-Border Transfers of Customer Personal Data. Customer authorizes Notion and its Subprocessors to transfer Customer Personal Data across international borders, including from the EEA, Switzerland, and/or the United Kingdom to the United States.

4.2 Standard Contractual Clauses. The parties agree that, when the transfer of Customer Personal Data from Customer to Notion is a Restricted Transfer, it shall be subject to the appropriate SCCs as follows:

4.2.1. in relation to Customer Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

i. Module Two will apply (where Customer is the Controller of Customer Personal Data), otherwise Module Three will apply (where Customer is a Processor of Customer Personal Data), as appropriate;

ii. in Clause 7, the optional docking clause will apply;

iii. in Clause 9, Option 2 will apply, and the time period for prior notice of subprocessor changes shall be as set out in Clause 3.5 of this DPA;

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 the laws of Ireland;

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 Annex I to this DPA;

viii. Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this DPA;

4.2.2. in relation to Restricted Transfers of Customer Personal Data protected by UK GDPR, the UK IDTA will apply completed as follows:

1. the IDTA will apply the EU SCCs (completed as set out in paragraph 4.2.1) to Restricted Transfers of Customer Personal Data from the UK;
2. Tables 1 – 3 of the UK IDTA shall be deemed completed with the relevant information set out in this DPA and the EU SCCs (completed as set out in paragraph 4.2.1 above);
3. Table 1 of the UK IDTA shall be deemed signed by Customer and Notion upon the entry into force of this DPA, and the start date specified in Table 1 of the UK DPA shall be deemed completed with the date of entry into force of this DPA;
4. In Table 4, the option “Importer” shall be deemed selected.

4.2.3. in relation to Customer Personal Data that is protected by the Data Protection Laws of Switzerland, then the EU SCCs will apply with the following modifications: the competent supervisory authority in Annex 1.C under Clause 13 will be the Federal Data Protection and Information Commissioner; references to a “Member State” and “EU Member State” will not be read to prevent data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland); and references to “GDPR” in the EU SCCs will be understood as references to Data Protection Laws of Switzerland.

4.2.4. in the event that any provision of this DPA contradicts the SCCs (directly or indirectly), the SCCs shall prevail.

4.2.5. The parties agree that, in the event where Data Protection Laws no longer allows the lawful transfer of Customer Personal Data to Notion and/or requires an alternative transfer solution that complies with Applicable Privacy Law(s), Notion will make an amendment to this DPA available to Customer to remedy such non-compliance and/or cease processing of Customer Personal Data without penalty.

5. Information Security Program

5.1 Security Measures. Notion shall implement and maintain commercially reasonable administrative, technical, and physical measures designed to protect Customer Personal Data as set forth in the Notion Security Standards. Notion regularly monitors compliance with these measures. Notion will not materially decrease the overall security of the Service during any Subscription Term.

6. Security Incidents.

6.1 Notice. Upon becoming aware of a Security Incident, Notion agrees to provide written notice to Customer without undue delay. Any such notification is not an acknowledgement of fault or responsibility. Where possible, such notice will include all details known to Notion and required under Data Protection Law(s) for Customer to comply with Customer's own notification obligations to regulatory authorities or individuals affected by the Security Incident, which may include, as applicable and if known, how the Security Incident occurred, the categories and approximate number of data subjects concerned, and the categories and approximate number of Customer Personal Data records concerned, the likely consequences of the Security Incident, and measures taken or proposed to be taken by Notion to address the Security Incident, including, where appropriate, measures designed to mitigate its possible adverse effects. Notion shall use commercially reasonable efforts to: (i) investigate and identify the cause of such Security Incident; (ii) remedy or mitigate the possible adverse effects of such Security Incidents, and (iii) reduce the likelihood that such Security Incident recurs. Notion will not assess the contents of Customer Personal Data in order to identify information subject to any specific legal requirements or assess the applicability of any specific privacy, data protection or cybersecurity requirement pertaining to such information. Customer is solely responsible for complying with Security Incident notification requirements applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident, provided that, at Customer's written request and subject to Customer paying Notion's reasonable fees (at then current rates) and expenses, Notion will provide Customer with assistance reasonably necessary to enable Customer to notify relevant security breaches to the competent data protection authorities and/or affected data subjects, if Customer is required to do so under Data Protection Law(s).

7. Audits

7.1 Third-Party Audit Reports. Notion obtains the third-party audits set forth in the Notion Security Standards. Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement and the entry into specific non-disclosure agreements, Notion shall make available to Customer (or Customer's independent, reputable, third-party auditor) information regarding Notion' compliance with the obligations set forth in this DPA by providing Customer with summaries of the most recent third-party audits reports referenced in the Notion Security Standards. All such summaries, to the extent not made generally publicly available by Notion on its website, constitute Notion's Confidential Information.

7.2 Audit of Notion. Where Data Protection Laws afford Customer an audit right, Customer (or Customer's independent, reputable, third-party auditor) may contact Notion in accordance with the "Notices" Section of the Agreement to request an audit of Notion' policies, procedures, and records relevant to the Processing of Customer Personal Data necessary to confirm Notion' compliance with this DPA, provided that the foregoing are within Notion' control and Notion is not precluded from disclosure by applicable law, a duty of confidentiality, or any other obligation owed to a third party. Customer shall reimburse Notion for its costs and expenses, including any time expended in connection with any such audit at Notion' then-current rates, which shall be made available to Customer upon request. Before the commencement of any such audit, Customer and Notion shall mutually agree upon the scope, timing, and duration of the audit, in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Notion. In no event shall Notion be required, in connection with any of its obligations under this DPA or otherwise, to provide information it is precluded from disclosing by applicable law, a duty of confidentiality, or any other obligation owed to a third party. Any audit must be: (i) conducted during Notion' regular business hours; (ii) with reasonable advance notice to Notion; (iii) carried out in a manner that prevents unnecessary disruption to Notion' operations; and (iv) subject to reasonable confidentiality procedures. In addition, any audit shall be limited to once per year, unless an audit is carried out at the direction of a government authority having proper jurisdiction. Customer shall promptly notify Notion of any alleged non-compliance with this DPA discovered during the course of an audit, and Notion shall use commercially reasonable efforts to address any confirmed non-compliance.

8. Data Deletion

8.1 Data Deletion. Upon termination or expiration of the Agreement, Notion shall, upon Customer's request, and subject to the limitations described in the Agreement and the Notion Security Standards, return to Customer (or make available for export in accordance with the Agreement) all Customer Personal Data in Notion' possession, or securely destroy such Customer Personal Data (excluding any back-up or archival copies which shall be deleted in accordance with Notion' data retention schedule), except where Notion is required to retain copies under applicable laws, in which case Notion will limit its processing of such Customer Personal Data except to the extent required by applicable laws.

9. Processing Details.

9.1 Subject Matter. The subject matter of the Processing is the Services pursuant to the Agreement.

9.2 Duration. Customer Personal Data will be Processed for the duration of the Agreement, including any post-termination retention period specified therein, subject to Section 8.1 of this DPA.

9.3 Categories of Data Subjects. Data subjects whose Customer Personal Data will be Processed pursuant to the Agreement may include Employees, Suppliers, Customers, Job Applicants, Consultants, and/or Contractors.

9.4 Nature and Purpose of the Processing. The nature and purpose of the Processing of Customer Personal Data by Notion is the performance of the Services pursuant to the Agreement. Customer acknowledges and agrees that it will not use the Services for any purposes deemed a “High Risk AI System” under the proposed EU Artificial Intelligence Act.

9.5 Types of Customer Personal Data. Customer represents and warrants to Notion that Customer Personal Data does not and will not contain, and Customer has not and will not otherwise provide or make available to Notion for Processing any sensitive personal data, including but not limited to financial information (e.g. credentials to any financial accounts or tax return data); health information (e.g. protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA) or other information regarding an individual's medical history, mental, or physical condition, or medical treatment or diagnosis by a health care professional, health insurance information, or genetic information); biometric information; government IDs or other government-issued identifiers (e.g. social security numbers); passwords for online accounts (other than passwords necessary to access the Services); credit reports or consumer reports; any payment card information or cardholder data subject to the Payment Card Industry Data Security Standard; information subject to the Gramm-Leach-Bliley Act, Fair Credit Reporting Act, or similar laws, or the regulations promulgated thereunder; information subject to restrictions under applicable law governing personal data of children, including, without limitation, all information about children under 16 years of age; or any information that falls within any special categories of data (as defined under the EU/UK Data Protection Law or otherwise interpreted under the implementing laws of the EEA member states).

Annex I - Data Processing Description

This Annex I forms part of the DPA and describes the processing that Notion (as the Processor or Subprocessor, as applicable) will perform on behalf of the Customer (as the Controller or Processor, as applicable).

A. LIST OF PARTIES

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

Name: *Customer listed in the applicable Order Form.*

Address: *Address listed in the applicable Order Form.*

Contact person's name, position and contact details: *Contact person listed in the applicable Order Form.*

Activities relevant to the data transferred under these Clauses: *Processing to carry out the Services pursuant to the Agreement entered into between Customer and Notion.*

Signature and date: *This Annex I shall automatically be deemed executed when Customer agrees to the Agreement.*

Role (controller/processor): *Controller or Processor, as applicable*

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

Name: *Notion Labs, Inc.*

Address: *2300 Harrison Street, Floor 2, San Francisco, CA 94110 USA*

Contact person's name, position and contact details: *Hasani Caraway, General Counsel, hasani@makenotion.com*

Activities relevant to the data transferred under these Clauses: *Processing to carry out the Services pursuant to the Agreement entered into between Customer and Notion.*

Signature and date: *This Annex I shall automatically be deemed executed when Customer agrees to the Agreement.*

Role (controller/processor): *Controller or Processor, as applicable*

B. DESCRIPTION OF PROCESSING/ TRANSFER

EU SCC Module: *C2P (Module 2)*

Categories of Data Subjects: *The personal data transferred may concern the following categories of data subjects set forth in Section 9.3 of the DPA:*

Employees, Suppliers, Customers, Job Applicants, Consultants, and Contractors

Purpose(s) of the data transfer and further processing/ processing operations: *The purpose of the transfer is the performance of the Services pursuant to the Agreement.*

Categories of Personal Data: *The personal data transferred concerns any category of personal data submitted by Customer to Notion pursuant to the Agreement, except for any personal data covered by Section 9.5 of the DPA.*

Sensitive data transferred (if applicable) and applied restrictions or safeguards: *As set forth in Section 9.5 of the DPA, sensitive data are expressly excluded from the scope of the Services.*

Frequency of the transfer: *Continuous*

Subject matter of the processing: *The subject matter of the Processing is Notion's Processing of Customer Personal Data to provide the Services pursuant to the Agreement.*

Nature and subject matter of the processing: *The nature and purpose of the transfer is the performance of the Services pursuant to the Agreement.*

Duration of the processing: *The duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.*

Retention period (or, if not possible to determine, the criterial used to determine the period): *For the duration of the Agreement. Upon termination of the Agreement, Customer Personal Data shall be returned or destroyed in accordance with Section 8.1 of the DPA.*

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs):

Where the EU GDPR applies, the supervisory authority is the EU Member State in which the Customer (or, if the Customer does not have an establishment in the EU, its representative) is established. Otherwise, if the Customer does not have an EU establishment nor an EU representative, the Irish Data Protection Commission.

Where the UK GDPR applies, the UK Information Commissioner's Office.

Annex II - Technical and Organisational Security Measures

Description of the technical and organisational measures implemented by the Processor(s) / Data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

1. **Measures of pseudonymisation and encryption of personal data**

   Notion encrypts data in transit via TLS 1.2, and at rest using the AES-256 algorithm.

2. **Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services**

   Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services include:

   Access to production systems is regulated through VPN, leveraging unique accounts and role-based access within operational and corporate environments. Authorization requests for access are tracked and logged on a regular basis. Removal of access for employees upon termination or change of role. Multi-factor Authentication (MFA) is required for access to critical and production resources. Strong passwords are required, never stored in clear text and are encrypted in transit and at rest.

   Mandatory security training for employees is required, covering data protection, confidentiality, social engineering, password policies and overall security responsibilities. Confidentiality requirements are imposed on employees. NDAs with third parties are required. Separation of networks based on trust levels are in place.

3. **Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident**

   Notion has processes in place to ensure ongoing confidentiality, availability and resilience to customer accounts and Customer Personal Data and during a security incident to help restore timely access to personal data following an incident.

4. **Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing**

   Notion performs annual penetration tests for all components of the Services, including web and mobile applications.

   Notion maintains security incident management policies and procedures. Notion notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by Notion or its sub-processors of which Notion becomes aware to the extent permitted by law.

5. **Measures for user identification and authorisation**

   The Services support SAML for Customers. Access to the Services by Notion personnel is uniquely identifiable, logged and monitored. Access to back-end infrastructure by Notion personnel requires multiple layers of authentication including requiring unique identifiers, optimal password strength and the use of Multi-factor Authentication.

6. **Measures for the protection of data during transmission**

   Notion employs TLS 1.2 encryption from the User’s browser to the Services, for Customer Data in transit.

7. **Measures for the protection of data during storage**

   Notion customer instances are logically separated and attempts to access data outside allowed domain boundaries are prevented and logged. Measures are in place to ensure executable uploads, code, or unauthorized actors are not permitted to access unauthorized data - including one customer accessing files of another customer.

8. **Measures for ensuring physical security of locations at which personal data are processed**

   Subprocessors are responsible for physical security of the data centers and are contractually obligated to ensure that physical security measures and resources are in place. These systems permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and