DATA PROCESSING AGREEMENT

Between the Controller and Nullbase ApS as Processor for the PasteBase Service

PREAMBLE

This Data Processing Agreement ("**DPA**" or "**Agreement**") is entered into between:

(1) The Controller — the legal entity or natural person identified in the Order Form, Service Agreement, or account registration details for the PasteBase service (hereinafter "**Controller**" or "**Customer**"); and

(2) Nullbase ApS, a private limited company registered under Danish law, with registered office at Rougsøvej 1, 8940 Randers SV, Denmark, CVR/VAT number DK37283681 (hereinafter "**Processor**" or "**PasteBase**").

Each individually a "**Party**" and together the "**Parties**".

This DPA supplements and forms an integral part of the Terms of Service available at https://pastebase.eu/terms/ ("**Main Agreement**") and takes effect on the date of the Controller's acceptance of the Main Agreement, or such later date as may be agreed in writing by the Parties ("**Effective Date**").

In the event of any conflict between this DPA and the Main Agreement with respect to the subject matter of data protection, this DPA shall prevail.

RECITALS

WHEREAS, the Processor provides a hosted paste and snippet management service ("**Service**") that enables the Controller to store, organise, and share reusable text content including email templates, code snippets, meeting notes, and similar materials;

WHEREAS, in the course of providing the Service, the Processor may process Personal Data on behalf of the Controller, including Personal Data that the Controller or its authorised team members may incorporate into paste content;

WHEREAS, Article 28(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**") requires that processing by a processor on behalf of a controller shall be governed by a binding contract or other legal act that sets out the subject matter, duration, nature, purpose, and type of Personal Data processed, and the obligations and rights of the controller;

WHEREAS, the Parties wish to enter into this DPA to ensure compliance with the GDPR and all applicable Data Protection Laws;

NOW, THEREFORE, in consideration of the mutual covenants set out herein, the Parties agree as follows.

ARTICLE 1 — DEFINITIONS

1.1 Unless otherwise defined herein, capitalised terms shall have the meanings set out below. Terms not defined here but used in the GDPR shall have the meanings ascribed to them in the GDPR.

(a) "Applicable Data Protection Law" means all laws and regulations applicable to the processing of Personal Data under this DPA, including but not limited to: the GDPR; the Danish Data Protection Act

legislation, binding guidance, codes of practice, or decisions issued by competent supervisory authorities.

(b) "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data, as defined in Article 4(7) GDPR. For the purposes of this DPA, the Controller is the Customer.

(c) "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed, within the meaning of Article 4(12) GDPR.

(d) "Data Subject" means an identified or identifiable natural person whose Personal Data is processed under this DPA.

(e) "EEA" means the European Economic Area, comprising all Member States of the European Union together with Norway, Iceland, and Liechtenstein.

(f) "Personal Data" means any information relating to an identified or identifiable natural person, as defined in Article 4(1) GDPR, that is processed by the Processor on behalf of the Controller under this DPA.

(g) "Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, as defined in Article 4(2) GDPR, including collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, dissemination, alignment, combination, restriction, erasure, or destruction.

(h) "Processor" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller, as defined in Article 4(8) GDPR. For the purposes of this DPA, the Processor is Nullbase ApS.

(i) "Restricted Transfer" means a transfer of Personal Data to a country or international organisation outside the EEA that has not been the subject of an adequacy decision by the European Commission pursuant to Article 45 GDPR.

(j) "Service" means the PasteBase hosted paste and snippet management platform provided by the Processor to the Controller pursuant to the Main Agreement.

(k) "Standard Contractual Clauses" or **"SCCs"** means the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR, as adopted by the European Commission by Decision 2021/914 of 4 June 2021, as may be amended or replaced by the European Commission from time to time.

(l) "Sub-processor" means any third party engaged by the Processor who processes Personal Data on behalf of the Processor in connection with the provision of the Service, as described in Article 6 of this DPA.

(m) "Supervisory Authority" means the competent data protection authority with jurisdiction over the Processor, being Datatilsynet (the Danish Data Protection Authority), or any other competent supervisory authority for the Controller under Applicable Data Protection Law.

(n) "Technical and Organisational Measures" means the measures described in Schedule 2 to this DPA and as further specified in Article 9.

ARTICLE 2 — SUBJECT MATTER, DURATION, NATURE, AND PURPOSE OF PROCESSING

2.1 Subject matter. The Processor shall process Personal Data on behalf of the Controller solely in connection with the provision, maintenance, and support of the Service, as more particularly described in Schedule 1 to this DPA.

2.2 Duration. The Processor shall process Personal Data for the duration of the Main Agreement, beginning on the Effective Date and continuing until the earlier of: (a) the termination or expiry of the Main Agreement; or (b) the completion of all post-termination obligations set out in Article 13 of this DPA ("**Processing Period**"). Obligations under this DPA that are expressed to survive termination shall remain in force after the end of the Processing Period.

2.3 Nature of processing. The nature of the processing comprises the following operations performed on Personal Data:

(a) Storage and retrieval of paste content and associated metadata within the Processor's infrastructure;

(b) Display, transmission, and rendering of paste content to authorised users of the Controller's team account;

(c) Logging of copy events (recording which user copied which paste and at what time) for the purpose of providing copy-count statistics within the Service dashboard;

(d) Sending of transactional emails (including team invitation emails) to email addresses provided by the Controller, via the Processor's authorised Sub-processor for email delivery;

(e) Authentication, access control, and session management for team members designated by the Controller;

(f) Backup, replication, and archival operations incidental to the secure operation of the database infrastructure.

2.4 Purpose of processing. The Processor processes Personal Data exclusively for the following purposes:

(a) Providing the Service in accordance with the Main Agreement;

(b) Enabling the Controller and its authorised team members to store, organise, access, and share paste content;

(c) Facilitating team collaboration through role-based access controls (Owner, Editor, and Member roles);

(d) Delivering transactional communications essential to the operation of the Service (email verification, team invitations, password reset);

(e) Maintaining the security, integrity, and availability of the Service;

(f) Complying with legal obligations applicable to the Processor.

The Processor shall not process Personal Data for any purpose other than those specified in this Article 2 or as otherwise instructed in writing by the Controller. The Processor shall not use Personal Data for its own commercial purposes, including marketing, advertising, profiling, or sale to third parties.

ARTICLE 3 — CATEGORIES OF PERSONAL DATA AND DATA SUBJECTS

3.1 Categories of Personal Data processed. Depending on the nature of the content the Controller and its team members store within the Service, the following categories of Personal Data may be processed under this DPA:

(a) Account and identity data of the Controller's team members (processed systematically):

- Full name and/or username
- Email address
- Hashed password credential
- Display name and optional biographical text
- Team membership role (Owner, Editor, Member)
- Email verification status and cryptographic verification token
- API access token (where generated by the user)
- Account creation and modification timestamps

(b) Operational and activity data (processed systematically):

- Session identifiers (stored as HttpOnly cookies, not logged to database)
- Copy event logs: user identifier, paste identifier, and timestamp of each copy action
- Invitation records: invitee email address, assigned role, inviting user identifier, invitation token, creation and expiry timestamps, and acceptance status

(c) Paste content (processed on the Controller's instructions; content and categories determined entirely by the Controller):

The Controller determines what text content is stored as pastes. Paste content may include, but is not limited to, personal data of third parties such as:

- Names, titles, and contact details of the Controller's clients, customers, employees, or partners
- Email addresses and telephone numbers referenced in email templates or notes
- Identification numbers or references used in business processes
- Any other personal data that the Controller incorporates into paste content in the course of its business operations

The Processor has no visibility into, control over, or responsibility for the categories of personal data that the Controller chooses to embed in paste content. The Controller bears sole responsibility as data controller for any personal data of third parties stored in paste content.

(d) Technical access data (processed incidentally, not systematically retained in application logs):

- IP addresses and user-agent strings transmitted by end-user browsers to the Processor's infrastructure in the ordinary course of HTTP communication

3.2 Categories of Data Subjects. Processing under this DPA may relate to the following categories of Data Subjects:

(a) Registered users of the Controller's PasteBase account, including the account Owner, Editors, and Members;

(b) Individuals invited by the Controller to join a team (whether or not they accept the invitation);

(c) Third parties whose personal data the Controller incorporates into paste content (e.g., names, email addresses, or contact details in email templates stored as pastes), the scope and categories of whom are determined solely by the Controller.

3.3 Sensitive categories of personal data. The Processor does not systematically process special categories of personal data within the meaning of Article 9 GDPR or personal data relating to criminal convictions and offences within the meaning of Article 10 GDPR. However, the Controller may, at its sole discretion, incorporate such categories of data into paste content. The Controller undertakes not to store special categories of personal data in paste content without implementing appropriate safeguards and without a lawful basis under Article 9(2) GDPR. Where the Controller does store such data, it remains the sole data controller responsible for compliance.

ARTICLE 4 — OBLIGATIONS OF THE PROCESSOR

4.1 Instructions. The Processor shall process Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country or an international organisation. The instructions of the Controller are set out in this DPA and in the Main Agreement. The Controller may issue further documented instructions in writing during the Processing Period. The Processor shall promptly inform the Controller if, in the Processor's opinion, an instruction infringes Applicable Data Protection Law, in which case the Processor may be entitled to suspend performance of the relevant instruction pending resolution.

4.2 Confidentiality. The Processor shall ensure that persons authorised to process Personal Data on the Processor's behalf are subject to binding and enforceable obligations of confidentiality with respect to Personal Data, or are under an appropriate statutory obligation of confidentiality. The Processor shall limit access to Personal Data to those personnel who require such access for the purposes of providing the Service.

4.3 Security. The Processor shall implement and maintain the Technical and Organisational Measures described in Article 9 and Schedule 2 of this DPA, and shall take all measures required pursuant to Article 32 GDPR, having regard to the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

4.4 Sub-processing. The Processor shall comply with Article 6 of this DPA with respect to the engagement of Sub-processors.

4.5 Data Subject rights. The Processor shall assist the Controller in accordance with Article 8 of this DPA.

4.6 Assistance with Controller obligations. Taking into account the nature of the processing and the information available to the Processor, the Processor shall assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR, including:

(a) Security of processing (Article 32 GDPR) — as set out in Article 9 and Schedule 2 of this DPA;

(b) Notification of Data Breaches to the supervisory authority (Article 33 GDPR) — as set out in Article 10 of this DPA;

(c) Communication of Data Breaches to Data Subjects (Article 34 GDPR) — as set out in Article 10 of this DPA;

(d) Data protection impact assessments (Article 35 GDPR) — by providing the Controller with such information as the Controller may reasonably require to conduct a DPIA with respect to the Service;

(e) Prior consultation with supervisory authorities (Article 36 GDPR) — by providing reasonable assistance and information to the Controller upon request.

4.7 Deletion or return. Upon termination or expiry of the Main Agreement, the Processor shall comply with Article 13 of this DPA.

4.8 Audit cooperation. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR, and shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller, in accordance with Article 12 of this DPA.

4.9 Notification of conflicting legal obligations. The Processor shall immediately inform the Controller if, in the Processor's opinion, an instruction given by the Controller would infringe Applicable Data Protection Law. Where the Processor is required by the law of a European Union Member State or by the law of a Member State applicable to the Processor to process Personal Data in a manner that deviates from the Controller's instructions, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.10 Records of processing activities. The Processor shall maintain, on behalf of the Controller, a record of all categories of processing activities carried out under this DPA, in accordance with Article 30(2) GDPR, and shall make this record available to the Supervisory Authority on request.

ARTICLE 5 — OBLIGATIONS OF THE CONTROLLER

5.1 Lawful basis. The Controller represents and warrants that it has a lawful basis under Article 6 GDPR (and, where applicable, Article 9 GDPR) for each processing activity instructed to the Processor under this DPA.

5.2 Controller instructions. The Controller shall ensure that its instructions to the Processor comply with Applicable Data Protection Law. The Controller shall notify the Processor promptly of any changes to its instructions that may affect the Processor's obligations under this DPA.

5.3 Data Subject rights. The Controller is responsible for responding to Data Subjects with respect to their rights under Articles 15 to 22 GDPR in relation to Personal Data processed under this DPA. The

Controller shall not direct Data Subjects to contact the Processor directly in the first instance without first notifying the Processor.

5.4 Content responsibility. The Controller is solely responsible for determining what content it stores within the Service. The Controller shall not store in paste content any Personal Data for which it does not have a lawful basis, nor shall it store special categories of Personal Data or data relating to criminal convictions without appropriate safeguards, and, where applicable, a specific legal basis under Article 9(2) GDPR.

5.5 Accuracy of data. The Controller is responsible for the accuracy, quality, and legality of the Personal Data it instructs the Processor to process.

5.6 Access management. The Controller is responsible for managing team memberships, user roles, and access permissions within the Service. The Controller shall promptly remove access for any team member who no longer requires it.

5.7 Compliance with applicable laws. Where the Controller is established outside the EEA, or where the Data Subjects are located outside the EEA, the Controller is responsible for ensuring compliance with any additional applicable data protection requirements beyond the GDPR.

ARTICLE 6 — SUB-PROCESSORS

6.1 General authorisation. The Controller grants the Processor general written authorisation to engage Sub-processors, subject to the conditions set out in this Article 6. The Processor shall maintain an up-to-date list of authorised Sub-processors, as set out in Schedule 3 to this DPA.

6.2 Obligations imposed on Sub-processors. Where the Processor engages a Sub-processor, the Processor shall impose on that Sub-processor, by way of a binding written contract, data protection obligations equivalent to those imposed on the Processor under this DPA. In particular, the Sub-processor shall provide sufficient guarantees to implement appropriate Technical and Organisational Measures such that the processing will meet the requirements of the GDPR.

6.3 Liability for Sub-processors. The Processor shall remain fully liable to the Controller for the performance of the Sub-processor's obligations to the extent that the Sub-processor fails to fulfil its data protection obligations. The engagement of Sub-processors does not relieve the Processor of any of its obligations under this DPA or under Applicable Data Protection Law.

6.4 Changes to Sub-processors. The Processor shall inform the Controller of any intended changes to Sub-processors, whether by addition or replacement, by providing the Controller with at least **thirty (30) calendar days'** prior written notice ("**Sub-processor Change Notice**"). The notice shall include the identity of the proposed Sub-processor, its country of establishment, and the nature of the processing to be carried out.

6.5 Objection to Sub-processors. The Controller may object to the Processor's use of a new or replacement Sub-processor on reasonable, documented data protection grounds by notifying the Processor in writing within **fourteen (14) calendar days** of receipt of a Sub-processor Change Notice. Where the Controller objects and the Processor cannot accommodate the objection, each Party shall have the right to terminate the relevant part of the Service, or the Main Agreement in its entirety, on

written notice, without liability to the other Party for such termination, other than for fees prepaid by the Controller for the unexpired term, which shall be refunded on a pro-rata basis.

6.6 Current Sub-processors. The Sub-processors currently authorised by the Controller are listed in Schedule 3 to this DPA.

ARTICLE 7 — INTERNATIONAL TRANSFERS OF PERSONAL DATA

7.1 EEA-based processing. The Processor's primary infrastructure, including its application servers and PostgreSQL database, is located entirely within the European Economic Area. All core Personal Data processed under this DPA (including account data, paste content, and activity logs) is stored and processed exclusively within the EEA and is not subject to Restricted Transfer by the Processor itself.

7.2 Transfers via Sub-processors. Certain Sub-processors listed in Schedule 3 are established outside the EEA and receive limited categories of Personal Data as described in Schedule 3. Restricted Transfers to such Sub-processors are made on the following bases:

(a) EU-US Data Privacy Framework. Where a Sub-processor is established in the United States and is certified under the EU-US Data Privacy Framework ("**DPF**") pursuant to the European Commission adequacy decision of 10 July 2023, the Restricted Transfer is made on the basis of that adequacy decision. The Processor shall verify and monitor the continued certification of such Sub-processors under the DPF.

(b) Standard Contractual Clauses. Where a Restricted Transfer cannot be made on the basis of an adequacy decision, the Processor shall ensure that the transfer is subject to the Standard Contractual Clauses or such other transfer mechanism as may be permitted under Chapter V GDPR.

(c) Other adequacy decisions. Where the European Commission has adopted an adequacy decision in respect of the destination country pursuant to Article 45 GDPR, the Processor may rely on that decision as the basis for the Restricted Transfer.

7.3 Transfer impact assessments. Where required by Applicable Data Protection Law or by the terms of the applicable transfer mechanism, the Processor shall conduct or cooperate in conducting a transfer impact assessment ("**TIA**") in respect of Restricted Transfers made by or on behalf of the Processor.

7.4 No new transfers. The Processor shall not instruct any Sub-processor to make Restricted Transfers of Personal Data to new destination countries without first providing the Controller with a Sub-processor Change Notice under Article 6.4 and implementing an appropriate transfer mechanism.

7.5 Controller-initiated transfers. Where the Controller itself transfers Personal Data to the Processor from outside the EEA, the Controller is responsible for ensuring that such transfer is made on an appropriate legal basis.

ARTICLE 8 — ASSISTANCE WITH DATA SUBJECT RIGHTS

8.1 General obligation. The Processor shall assist the Controller in fulfilling the Controller's obligations to respond to requests from Data Subjects exercising their rights under Chapter III GDPR (Articles 15 to 22), including:

(a) Right of access (Article 15);

(b) Right to rectification (Article 16);

(c) Right to erasure ("right to be forgotten") (Article 17);

(d) Right to restriction of processing (Article 18);

(e) Right to data portability (Article 20);

(f) Right to object (Article 21);

(g) Rights in relation to automated individual decision-making (Article 22).

8.2 Data Subject requests received by the Processor. Where the Processor receives a request from a Data Subject purporting to exercise rights under Chapter III GDPR in relation to Personal Data processed under this DPA, the Processor shall:

(a) Without undue delay, and in any event within **five (5) business days** of receipt, inform the Controller of the request;

(b) Not respond substantively to the request without written authorisation from the Controller, unless required to do so by Applicable Data Protection Law;

(c) At the Controller's direction, provide reasonable assistance to the Controller in formulating its response.

8.3 Technical assistance. Having regard to the nature of the processing and the Technical and Organisational Measures implemented, the Processor shall provide reasonable technical and administrative assistance to enable the Controller to:

(a) Locate and extract Personal Data relating to a specific Data Subject from the Service upon the Controller's written request;

(b) Implement restrictions on the processing of a specific Data Subject's Personal Data upon the Controller's written instruction;

(c) Erase or anonymise Personal Data relating to a specific Data Subject upon the Controller's written instruction;

(d) Provide the Controller with a structured, commonly used, machine-readable export of a Data Subject's Personal Data processed under this DPA.

8.4 Costs. The Processor shall provide reasonable assistance under this Article 8 at no additional charge where such assistance is proportionate to the request. Where a request requires disproportionate effort or resource, the Processor shall notify the Controller and the Parties shall agree in good faith on reasonable compensation for such additional work.

ARTICLE 9 — TECHNICAL AND ORGANISATIONAL MEASURES (ARTICLE 32 GDPR)

9.1 General standard. The Processor shall implement and maintain Technical and Organisational Measures appropriate to the risk presented by the processing under this DPA, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons pursuant to Article 32(1) GDPR.

9.2 Specific measures. The Technical and Organisational Measures currently implemented by the Processor are described in Schedule 2 to this DPA. These measures include at a minimum:

(a) Encryption and transport security:

- All communications between end-user clients and the Service are encrypted using TLS (Transport Layer Security), enforced via HTTP Strict Transport Security (HSTS) headers with a minimum max-age of 31,536,000 seconds (one year), including subdomains, with HSTS preload enabled;

(b) Password and credential security:

- User passwords are never stored in plain text; they are hashed using Django's default PBKDF2-HMAC-SHA256 algorithm with a cryptographically random salt;
- All security-sensitive tokens (email verification tokens, invitation tokens, password reset tokens, and API access tokens) are generated using cryptographically secure pseudo-random number generators (`secrets.token_urlsafe(32)` in Python, yielding a minimum of 256 bits of entropy);

(c) Session and cookie security:

- Session cookies (`sessionid`) are marked HttpOnly (inaccessible to JavaScript) and SameSite=Lax in all environments, and Secure (HTTPS-only) in production;
- CSRF tokens (`csrftoken`) are marked HttpOnly and applied to all state-changing requests via Django's built-in CSRF middleware;

(d) Application security:

- Cross-Site Request Forgery (CSRF) protection applied to all POST, PUT, PATCH, and DELETE requests;
- Clickjacking protection via X-Frame-Options header;
- Django's SecurityMiddleware provides additional security headers;

(e) Access controls:

- Role-based access control (RBAC) with three defined roles: Owner, Editor, and Member;
- Team content is accessible only to authenticated members of the relevant team;
- Email verification is required before any authenticated access to the Service is granted (enforced at the middleware layer);

(f) Infrastructure security:

- Application and database servers are located exclusively within the EEA;
- The PostgreSQL database is not exposed to the public internet; it is accessible only within the private Docker network of the application stack;
- Database credentials are managed via environment variables and are not embedded in source code;

(g) Availability and integrity:

- Persistent data is stored in named Docker volumes to prevent inadvertent data loss;
- Database backups are taken in accordance with the Processor's operational procedures;

(h) Organisational measures:

- Access to production systems is restricted to authorised personnel of the Processor on a need-to-know basis;

- Personnel with access to Personal Data are bound by confidentiality obligations;
- The Processor maintains an internal Data Breach register.

9.3 Adaptation of measures. The Processor shall regularly review the Technical and Organisational Measures and update them as necessary to ensure a level of security appropriate to the risk. The Processor shall notify the Controller of any material reduction in the level of security implemented.

9.4 No guarantee. The Processor does not guarantee absolute security. The obligation is to implement measures appropriate to the risk, in accordance with Article 32(1) GDPR.

ARTICLE 10 — DATA BREACH NOTIFICATION

10.1 Processor's notification obligation to Controller. Without undue delay, and in any event no later than **forty-eight (48) hours** after becoming aware of a Data Breach affecting Personal Data processed under this DPA, the Processor shall notify the Controller. The notification shall, to the extent possible at the time of notification, include the following information:

(a) A description of the nature of the Data Breach, including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

(b) The name and contact details of the Processor's data protection contact point from whom more information can be obtained;

(c) A description of the likely consequences of the Data Breach;

(d) A description of the measures taken or proposed to be taken by the Processor to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

10.2 Phased notification. Where full information is not available within the forty-eight (48) hour period, the Processor shall provide an initial notification within that period with such information as is available, and shall provide further updates as additional information becomes available, without undue further delay.

10.3 Controller's notification obligations. The Controller is responsible for:

(a) Notifying the competent Supervisory Authority of a Data Breach, where required by Article 33 GDPR, within **seventy-two (72) hours** of becoming aware of it (taking into account that the Processor's forty-eight (48) hour notification period is designed to allow the Controller time to assess the breach and prepare its notification);

(b) Communicating the Data Breach to affected Data Subjects where required by Article 34 GDPR.

10.4 Processor's assistance. The Processor shall provide the Controller with all reasonable assistance in connection with the Controller's notification obligations under Articles 33 and 34 GDPR, including by promptly answering questions, providing additional information, and cooperating with any investigation.

10.5 Processor's contact. All notifications from the Processor to the Controller under this Article 10 shall be made to the email address associated with the Controller's account, and shall copy: support@pastebase.eu.

10.6 Breach register. The Processor shall maintain an internal record of all Data Breaches in accordance with Article 33(5) GDPR, regardless of whether notification to the Supervisory Authority is required, and shall make this record available to the Controller upon request.

10.7 Responsibility for notification costs. Each Party shall bear its own costs in connection with Data Breach investigation, remediation, and notification, except that where a Data Breach is caused by the Controller's instructions or by Personal Data provided by the Controller, the Controller shall bear all reasonable costs incurred by the Processor in connection with that breach.

ARTICLE 11 — DATA PROTECTION IMPACT ASSESSMENTS AND PRIOR CONSULTATION

11.1 Assistance with DPIAs. Where the Controller is required to carry out a Data Protection Impact Assessment ("**DPIA**") pursuant to Article 35 GDPR in relation to the processing under this DPA, the Processor shall, upon the Controller's written request, provide the Controller with reasonable assistance, including by making available to the Controller such information concerning the Processor's processing operations, Technical and Organisational Measures, and Sub-processor arrangements as the Controller may reasonably require to complete the DPIA.

11.2 Prior consultation. Where a DPIA indicates that processing would result in a high risk in the absence of measures taken by the Controller, the Controller shall consult the competent Supervisory Authority prior to the processing in accordance with Article 36 GDPR. The Processor shall provide the Controller with reasonable assistance in preparing for such consultation.

11.3 No obligation to conduct DPIAs. Nothing in this Article 11 obliges the Processor to conduct a DPIA on behalf of the Controller, which remains the Controller's responsibility. The Processor's obligation is limited to providing reasonable assistance as described above.

ARTICLE 12 — AUDIT RIGHTS AND INFORMATION

12.1 Information obligation. The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and in this DPA. The Processor shall maintain accurate and up-to-date records of its processing activities carried out on behalf of the Controller in accordance with Article 30(2) GDPR.

12.2 Audit right. The Controller or an auditor mandated by the Controller shall have the right to conduct audits, including on-site inspections, of the Processor's processing operations to verify compliance with this DPA and Applicable Data Protection Law, subject to the conditions in this Article 12.

12.3 Conditions for audits.

(a) The Controller shall give the Processor **thirty (30) calendar days'** prior written notice of an intended audit, specifying the scope, proposed dates, and the identity of any mandated auditor;

(b) Audits shall be conducted during normal business hours, at reasonable frequency (not more than once per calendar year, unless a Data Breach or supervisory authority investigation requires otherwise), and in a manner that minimises disruption to the Processor's operations;

(c) The mandated auditor must not be a competitor of the Processor and must agree in writing to comply with the Processor's reasonable confidentiality requirements before commencing the audit;

(d) The Controller shall bear all costs and expenses associated with the audit, unless the audit reveals material non-compliance by the Processor, in which case the Processor shall bear the reasonable costs of the audit.

12.4 Third-party certifications. Where the Processor has obtained a third-party audit report, certification, or attestation (such as ISO 27001 or SOC 2) relevant to the subject matter of this DPA, the Processor shall, upon request, make such reports available to the Controller in lieu of, or to reduce the scope of, an on-site audit.

12.5 Supervisory authority access. Nothing in this Article 12 shall limit the right of a Supervisory Authority to conduct audits or inspections of the Processor pursuant to Article 58 GDPR.

ARTICLE 13 — DELETION AND RETURN OF PERSONAL DATA ON TERMINATION

13.1 Post-termination obligations. Upon the termination or expiry of the Main Agreement for any reason, the Processor shall, at the Controller's election (to be communicated in writing to the Processor no later than thirty (30) calendar days after the date of termination):

(a) **Return:** Provide the Controller with an export of all Personal Data processed under this DPA, in a structured, commonly used, and machine-readable format (such as JSON or CSV), within thirty (30) calendar days of the Controller's written request; and/or

(b) **Delete:** Securely and irreversibly delete or destroy all Personal Data processed under this DPA (including all copies and backups), within sixty (60) calendar days of the date of termination, and provide the Controller with written confirmation of deletion upon request.

13.2 Default deletion. Where the Controller does not make an election under Article 13.1 within thirty (30) calendar days after termination, the Processor shall proceed with secure deletion of all Personal Data in accordance with Article 13.1(b).

13.3 Legal retention obligations. Notwithstanding Article 13.1 and 13.2, the Processor may retain Personal Data to the extent and for the duration required by Applicable Data Protection Law or by other applicable EU or Member State law. Where the Processor retains Personal Data pursuant to this Article 13.3, it shall notify the Controller of the legal basis for retention, the categories of data retained, and the retention period, and shall continue to apply the obligations of this DPA to such retained data.

13.4 Sub-processor deletion. The Processor shall ensure that Sub-processors are subject to equivalent deletion obligations and shall procure that Sub-processors delete Personal Data in accordance with this Article 13 following termination.

13.5 Costs. The Processor shall provide a data export under Article 13.1(a) at no additional charge for the first request following termination. The Controller shall bear the cost of any additional exports, at the Processor's then-prevailing rates.

ARTICLE 14 — LIABILITY

14.1 General liability. Each Party's liability to the other Party under this DPA shall be subject to the limitations and exclusions set out in the Main Agreement.

14.2 Liability to Data Subjects and supervisory authorities. The allocation of liability between the Parties for Data Subject claims and regulatory penalties shall be as follows:

(a) Where a Data Subject has suffered damage as a result of processing in infringement of the GDPR, and both Parties are responsible for such infringement, each Party shall be held liable for the entire damage in accordance with Article 82(4) GDPR; however, either Party may be exempted from liability to the extent it proves that it is not in any way responsible for the event giving rise to the damage in accordance with Article 82(3) GDPR;

(b) Where the Processor has paid full compensation to a Data Subject, the Processor shall be entitled to claim back from the Controller that part of the compensation corresponding to the Controller's part of responsibility for the damage, and vice versa;

(c) Administrative fines imposed by a Supervisory Authority shall be borne by the Party to whom the fine is directed, subject to any rights of contribution between the Parties where the fine was caused by or contributed to by the other Party's breach of this DPA.

14.3 Mutual indemnity. Each Party ("**Indemnifying Party**") shall indemnify, defend, and hold harmless the other Party ("**Indemnified Party**") from and against any claims, damages, losses, penalties, costs, and expenses (including reasonable legal fees) arising from the Indemnifying Party's breach of this DPA or of Applicable Data Protection Law, to the extent such breach caused or contributed to the loss or liability of the Indemnified Party, subject always to the liability limitations in the Main Agreement.

14.4 Processor indemnity. Without limiting Article 14.3, the Processor shall indemnify the Controller for any regulatory fines, Data Subject compensation awards, or third-party claims arising directly from the Processor's: (a) processing of Personal Data in breach of the Controller's documented instructions; (b) failure to implement the Technical and Organisational Measures described in Schedule 2; or (c) failure to comply with its Sub-processor obligations under Article 6.

14.5 Controller indemnity. Without limiting Article 14.3, the Controller shall indemnify the Processor for any regulatory fines, Data Subject compensation awards, or third-party claims arising directly from: (a) the Controller's instructions being in breach of Applicable Data Protection Law; (b) the Controller's failure to obtain a lawful basis for the processing instructed to the Processor; or (c) the Controller storing Personal Data in paste content in violation of Article 3.3 or Article 5.4 of this DPA.

ARTICLE 15 — GENERAL PROVISIONS

15.1 Order of precedence. In the event of any conflict or inconsistency between the provisions of this DPA and any other document forming part of the agreement between the Parties, this DPA shall prevail in respect of data protection matters.

15.2 Severability. If any provision of this DPA is found to be invalid, illegal, or unenforceable by a court of competent jurisdiction or by a Supervisory Authority, such provision shall be modified to the minimum

extent necessary to make it valid and enforceable, and the validity and enforceability of the remaining provisions shall not be affected.

15.3 Amendments. This DPA may be amended only by a written instrument signed by authorised representatives of both Parties. Where amendment is required by a change in Applicable Data Protection Law or by a decision of a Supervisory Authority or court, the Processor may propose an amendment by giving the Controller thirty (30) calendar days' notice in writing. Where the Controller does not accept the proposed amendment, the Parties shall negotiate in good faith.

15.4 Assignment. This DPA may not be assigned by either Party without the prior written consent of the other Party, except that the Processor may assign this DPA to an affiliate or successor entity in connection with a merger, acquisition, or sale of all or substantially all of its assets, provided that: (a) the Controller is notified in writing at least thirty (30) calendar days in advance; (b) the assignee assumes all obligations of the Processor under this DPA; and (c) the level of data protection is not reduced.

15.5 No waiver. Failure by either Party to enforce any provision of this DPA shall not constitute a waiver of that provision or any other provision, or of the right to enforce any provision in the future.

15.6 Entire agreement. This DPA, together with the Main Agreement and all Schedules hereto, constitutes the entire agreement between the Parties with respect to the processing of Personal Data under the Service, and supersedes all prior agreements, representations, and understandings between the Parties relating to such subject matter.

15.7 Counterparts. This DPA may be executed in counterparts (including by electronic signature), each of which shall be deemed an original and all of which together shall constitute one and the same instrument. An electronic acceptance of the Main Agreement that incorporates this DPA by reference shall constitute valid execution.

15.8 Language. This DPA is made in the English language. In the event of any inconsistency between an English version and any translation, the English version shall prevail.

15.9 Governing law. This DPA shall be governed by and construed in accordance with the laws of Denmark, without regard to its conflict of laws principles. The courts of Denmark shall have exclusive jurisdiction over any dispute arising from or in connection with this DPA, subject to the right of either Party to seek urgent interim relief from any competent court. EU consumer protection rules that are mandatory in the Controller's jurisdiction of residence shall not be excluded by this provision where the Controller is an individual consumer.

15.10 Supervisory authority. The lead supervisory authority for the Processor is:

Datatilsynet (Danish Data Protection Authority)

Carl Jacobsens Vej 35

2500 Valby, Denmark

Tel: +45 33 19 32 00

Email: dt@datatilsynet.dk

Website: datatilsynet.dk

15.11 Contact. All notices and communications under this DPA shall be made in writing to:

Processor: Nullbase ApS, Rougsøvej 1, 8940 Randers SV, Denmark; Email: support@pastebase.eu; Tel: +45 70 60 60 02

Controller: The email address and contact details provided in the Controller's account registration or as updated by the Controller from time to time.

SCHEDULE 1 — DESCRIPTION OF PROCESSING

This Schedule sets out the details of the processing carried out by the Processor on behalf of the Controller, pursuant to Article 28(3) GDPR.

1. Subject matter of processing

The provision, operation, maintenance, and support of the PasteBase hosted paste and snippet management service, enabling the Controller to store, organise, access, share, and copy text-based content items ("pastes") within team workspaces.

2. Duration of processing

From the Effective Date of the DPA until sixty (60) calendar days after the termination or expiry of the Main Agreement (to allow for the data export and deletion procedures under Article 13).

3. Nature and purpose of the processing

Processing operation	Purpose
Storage of paste content (title, category, editor type, code language, content text) in PostgreSQL database	Enabling the Controller's authorised users to retrieve and copy reusable text content
Storage of account and profile data (username, email, hashed password, display name, bio)	Authentication, authorisation, and account management
Storage of team and membership data (team name, slug, membership role, join date)	Enabling role-based collaborative access to shared paste collections
Storage of invitation records (invitee email, role, token, expiry, status)	Enabling the Controller to invite colleagues to team workspaces
Storage of copy event logs (user ID, paste ID, copy timestamp)	Providing usage statistics to the Controller within the Service dashboard
Storage of email verification tokens	Verifying that account email addresses belong to the registering user
Storage of API access tokens	Enabling programmatic access to the Service for authorised users
Transmission of email addresses to the email Sub-processor (Resend)	Delivering transactional emails (verification, invitation, password reset)
Transmission of IP addresses and user-agent strings to CDN Sub-processors	Delivering web fonts and CSS framework assets required for the Service UI

4. Types of personal data

- **Identity and contact data:** Username, email address, display name, bio
- **Credential data:** Hashed passwords (PBKDF2-HMAC-SHA256; irreversible), cryptographic tokens
- **Membership and role data:** Team membership, assigned role, join date
- **Activity data:** Copy event logs (user, paste, timestamp)
- **Invitation data:** Invitee email address, invited-by user, role, dates
- **Paste content:** Free-form text determined by the Controller, which may contain personal data of third parties

5. Categories of Data Subjects

- Registered users of the Controller's PasteBase account (employees, contractors, or other individuals authorised by the Controller)
- Individuals invited to join the Controller's team
- Third parties whose personal data the Controller incorporates into paste content

6. Special categories of personal data

The Processor does not systematically process special categories of personal data. The Controller may, at its own discretion and responsibility, incorporate special category data into paste content.

7. Frequency of processing

Continuous and ongoing during the Processing Period, triggered by user actions (login, paste creation/editing, copying, invitations) or by automated system operations (session management, backup).

SCHEDULE 2 — TECHNICAL AND ORGANISATIONAL MEASURES

This Schedule describes the Technical and Organisational Measures ("TOMs") implemented by the Processor as of the Effective Date of this DPA, pursuant to Article 32 GDPR and Article 9 of the DPA.

A. Measures of pseudonymisation and encryption

Measure	Implementation
Transport encryption	TLS enforced on all HTTP connections; HSTS header with max-age 31,536,000 seconds, includeSubDomains, and preload directives
Password hashing	PBKDF2-HMAC-SHA256 with unique cryptographic salt per password (Django default hasher); passwords are never stored in recoverable form
Token generation	All security tokens (verification, invitation, password reset, API access) generated via Python `secrets.token_urlsafe(32)` — minimum 256 bits of entropy
Database encryption at rest	Implemented at infrastructure level per the Processor's hosting provider's standard practice

B. Measures for ensuring ongoing confidentiality, integrity, availability, and resilience

Measure	Implementation
Data isolation	Each team's pastes are scoped to that team; cross-team access is not possible
Database access isolation	PostgreSQL is not exposed to the public internet; accessible only within the private container network
Session security	Session cookies: HttpOnly=true, SameSite=Lax, Secure=true (production); CSRF tokens: HttpOnly=true
CSRF protection	Django CsrfViewMiddleware applied to all state-changing requests
Clickjacking protection	X-Frame-Options header enforced by Django's XFrameOptionsMiddleware
Email verification gate	EmailVerificationMiddleware blocks all authenticated access until email is verified; superuser accounts are exempt
Availability	Persistent storage in named Docker volumes protected from inadvertent deletion; database separated from application container
Backup	Database backup procedures maintained operationally by the Processor

C. Measures for ensuring the ability to restore availability and access to personal data

Measure	Implementation
Database persistence	Data stored in `pgdata` Docker volume; application explicitly documented to never use `docker compose down -v`
Static file persistence	Static assets stored in separate `staticfiles` Docker volume
Backup and recovery	Operational backup procedures; recovery tested periodically

D. Processes for regular testing, assessing, and evaluating effectiveness

Measure	Implementation
Dependency management	Python dependencies managed via requirements files; updated as security patches are released
Framework security	Relies on Django's well-maintained security framework including regular upstream security patches
Access review	Team membership and roles reviewed by the Controller as Owner of the team
Breach register	Internal breach register maintained by the Processor

E. Measures for user identification and authorisation

Measure	Implementation
Authentication	Username and password authentication; email verification required
Role-based access control	Three-tier role model: Owner (full control), Editor (create/edit/delete pastes), Member (view/copy pastes)
Token-based access	Optional API access token for programmatic access; token revocable by the user at any time
Invitation expiry	Team invitations expire automatically after 3 days and become invalid upon expiry

F. Measures for the protection of data during transmission

Measure	Implementation
In-transit encryption	TLS on all connections between client and server
HSTS preload	Browsers instructed to use HTTPS exclusively for the domain
Secure cookies	Session and CSRF cookies transmitted only over HTTPS in production

G. Measures for the protection of data during storage

Measure	Implementation
Hashed passwords	Passwords stored as irreversible hashes only
Token rotation	Verification tokens generated fresh at each request
No logging of sensitive data	Passwords and plain-text tokens are never written to application logs

H. Measures for ensuring physical security

Physical security is managed by the Processor's EU-based infrastructure and hosting provider. The Processor's application runs in containerised infrastructure within EU-located data centres operated by the hosting provider. Physical access to underlying hardware is controlled by the hosting provider in accordance with their security policies.

I. Measures for ensuring events logging

Application-level events (copy logs, authentication events) are stored in the application database. Infrastructure-level logs are maintained at the hosting provider level. The Processor maintains an internal breach register.

J. Measures for ensuring system configuration

Measure	Implementation
Secrets management	All secrets (database credentials, API keys, Django secret key) injected via environment variables; not stored in source code
Debug mode	DJANGO_DEBUG disabled in production
Minimal attack surface	No analytics, tracking, advertising, or unnecessary third-party integrations

K. Measures for minimisation of data

Measure	Implementation
No analytics	No web analytics, page-view tracking, or behavioural profiling implemented
No advertising	No advertising networks or data brokers used
Minimal cookies	Only technically necessary and user-preference cookies used; no tracking or advertising cookies
Minimal sub-processors	Sub-processors limited to those strictly necessary to operate the Service

SCHEDULE 3 — LIST OF AUTHORISED SUB-PROCESSORS

This Schedule lists all Sub-processors authorised by the Controller as of the Effective Date of this DPA, pursuant to Article 6 of the DPA.

Sub-processor	Legal entity and address	Country	Purpose	Data transferred	Transfer mechanism
Resend	Resend Inc., 2261 Market Street #5275, San Francisco, CA 94114, USA	United States	Transactional email delivery (account verification, team invitations, password reset)	Recipient email address; email subject line and body content	EU-US Data Privacy Framework (adequacy decision of 10 July 2023); Resend Standard Contractual Clauses
Google Fonts	Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	United States	Web font delivery (Plus Jakarta Sans typeface loaded from fonts.googleapis.com / fonts.gstatic.com)	End-user IP address; browser user-agent string	EU-US Data Privacy Framework (adequacy decision of 10 July 2023)

Sub-processor	Legal entity and address	Country	Purpose	Data transferred	Transfer mechanism
jsDelivr	Prospect One sp. z o.o., ul. Królewska 65a/1, 30-081 Kraków, Poland	Poland (EU)	CDN delivery of PicoCSS framework assets	End-user IP address; browser user-agent string	No Restricted Transfer — EU-based processor

Notes to Schedule 3:

1. The Processor shall notify the Controller of any changes to this Schedule 3 in accordance with Article 6.4 of this DPA, with a minimum of thirty (30) calendar days' notice.

2. With respect to **Resend**: Resend processes only the minimum data necessary to deliver transactional emails. Email content transmitted to Resend consists solely of system-generated transactional messages (verification links, invitation links, password reset links). No paste content is transmitted to Resend.

3. With respect to **Google Fonts**: Google Fonts is loaded client-side directly by the end-user's browser. The IP address and user-agent string are transmitted by the end-user's browser to Google's servers in the ordinary course of loading the web page. The Processor has no control over this transmission. The Controller acknowledges this processing and, where required, shall include appropriate information in its own privacy notices to Data Subjects.

4. With respect to **jsDelivr**: jsDelivr is operated by a Polish entity and processes data exclusively within the EU. No Restricted Transfer mechanism is required.

5. The Processor's primary hosting infrastructure (application server and PostgreSQL database) is operated within the EU and is not listed as a Sub-processor as it is operated directly by the Processor.

SCHEDULE 4 — STANDARD CONTRACTUAL CLAUSES (RESERVED)

Where a Restricted Transfer of Personal Data from the EEA to a third country is required under this DPA and an adequacy decision is not available or ceases to apply, the transfer shall be governed by the Standard Contractual Clauses as adopted by the European Commission in Decision 2021/914 of 4 June 2021, with Module Two (Controller to Processor) applying between the Controller (as data exporter) and the Processor (as data importer) for any transfers made by the Processor, or Module Three (Processor to Processor) applying between the Processor (as data exporter) and the relevant Sub-processor (as data importer).

This Schedule 4 is reserved for the incorporation of the applicable SCCs by amendment, where required.

SIGNATURE BLOCK

This Data Processing Agreement is entered into by the authorised representatives of the Parties as set forth below.

PROCESSOR

Nullbase ApS

Rougsøvej 1

8940 Randers SV

Denmark

CVR: DK37283681

Signed by: _____

Name: _____

Title: _____

Date: _____

Email: support@pastebase.eu

Tel: +45 70 60 60 02

CONTROLLER

Company / Trading name: _____

Registered address: _____

_____

Registration number (if applicable): _____

Signed by: _____

Name: _____

Title: _____

Date: _____

Email: _____

Tel: _____

This Data Processing Agreement is entered into for the purposes of Article 28(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) and constitutes a binding legal obligation on both Parties.

This DPA may be executed electronically. Acceptance of the PasteBase Terms of Service, which incorporates this DPA by reference, constitutes the Controller's agreement to the terms of this DPA.

Document control:

Version: 1.0

Effective date: 2 April 2026

Governing law: Kingdom of Denmark

Language: English