Data Processing Agreement according to Art. 28 GDPR

between

you

(hereinafter “Controller”)

and

heylogin GmbH
Sophienstr. 40
38118 Braunschweig
(hereinafter “Processor”),

collectively referred to as the “Parties”.

Preamble

The Controller and the Processor have concluded a framework agreement on the use of the password management system heylogin. For this purpose it is necessary that the Processor processes personal data on behalf of the Controller.

The Processor has appointed an external data protection officer:

Projekt 29 GmbH & Co. KG
Ostengasse 14
93047 Regensburg
Email: privacy@heylogin.com

Having said this, the Parties hereby enter into the following Agreement on Commissioned Processing pursuant to Article 28 of the GDPR (hereinafter: “Agreement”):

1 Subject of the data processing

1. The subject matter and duration of the data processing as well as the type and purpose of the processing result from the framework agreement and the service descriptions - which depend on the commissioned services. As a rule, the Processor processes the following data for the Controller:

    - **Stored data in heylogin (e.g. usernames, passwords, website URLs)**

  - **Nature and purpose of processing:** password management. The data is transmitted and stored exclusively with end-to-end encryption. Decryption or any processing in plain text is not technically possible for the processor. The processor is limited to the secure synchronization of encrypted data between the client's devices. A detailed list of the end-to-end encrypted data can be found in the heylogin security whitepaper in the section "What we encrypt and how" (see https://www.heylogin.com/en/whitepaper).
  - **Categories of data subjects:** users of heylogin
- **Account and organization data**
  - **Nature and purpose of processing:** management of accounts based on the email address as well as assignment to one or more heylogin organizations. This data is used exclusively for authentication and license management.
  - **Categories of data subjects:** users of heylogin
- **Log and metadata**
  - **Nature and purpose of processing:** processing of technical logs and metadata (e.g. login timestamps, technical logs, IP addresses) exclusively for the purposes of system security, abuse detection, and error analysis.
  - **Categories of data subjects:** users of heylogin
- **Support and device data**
  - **Nature and purpose of processing:** processing of device data as well as content voluntarily submitted in the course of support (e.g. screenshots, attachments, text information) exclusively for troubleshooting and support. No further use or analysis is carried out.
  - **Categories of data subjects:** users of heylogin

2. The duration of this data processing corresponds to the term of the framework agreement.
3. Processing includes collecting, arranging, storing, reading, using, transmitting and deleting personal data.

2 Scope of application and responsibility

1. The Processor shall process personal data on behalf of the Controller. This includes activities that are specified in the framework agreement and in the associated service descriptions. Within the scope of this contract, the Controller shall be solely responsible for compliance with the statutory provisions of the data protection laws, in particular for the lawfulness of the transfer of data to the Processor as well as for the lawfulness of the data processing ("Responsible Party" within the meaning of Art. 4 No. 7 GDPR).

2. The instructions shall initially be stipulated by the Contract and may thereafter be amended, supplemented or replaced by the Controller in writing or in an electronic format (text form) to the body designated by the Processor by means of individual instructions (individual instructions). Instructions not provided for in the contract shall be treated as a request for a change in performance. Verbal instructions shall be confirmed immediately in writing or in text form.

3 Rights and obligations of the Controller

1. The Controller is the responsible party pursuant to Art. 4 No. 7 GDPR for the processing of data on behalf of the Processor. As such, he must inform his employees about which data he collects and forwards to the Processor.
2. The Controller shall inform the Processor immediately and in full if it discovers errors or irregularities in the results of the order with regard to data protection regulations.
3. The Controller shall name the Processor the contact person for data protection issues arising within the scope of the contract.
4. If the Controller is held liable by a data subject for any claims under Art. 82 GDPR, the Processor agrees to support the Controller in defending against the claim to the best of its ability.

4 Duties of the Processor

1. The Processor may only process data of data subjects within the scope of the order and the Controller's instructions unless there is an exceptional case within the meaning of Article 28 (3) a) of the GDPR. The Processor shall inform the Controller without undue delay if it is of the opinion that an instruction violates applicable laws. The Processor may suspend the implementation of the instruction until it has been confirmed or amended by the Controller.
2. The Processor shall design the internal organization in its area of responsibility in such a way that it meets the special requirements of data protection. The Processor shall take technical and organizational measures for the adequate protection of the Controller's data which meet the requirements of the General Data Protection Regulation (Art. 32 GDPR) and ensure that the confidentiality, integrity, availability and resilience of the systems and services in connection with the processing are permanently guaranteed. The Principal is aware of these technical and organizational measures and is responsible for ensuring that they provide an adequate level of protection for the risks of the data to be processed.

3. A current list of technical and organizational measures is provided as an **annex** to this contract.
4. The Processor may change or update these measures at its own discretion, provided that these changes or updates correspond to the respective state of the art and the legal requirements, and the previous, contractually agreed level of protection is not undercut. The Processor shall inform the Controller of any significant changes or updates to the measures.
5. The Processor shall inform the Controller immediately if it has reason to believe that the technical and organizational measures are no longer sufficient to maintain the contractually agreed level of protection and shall then coordinate further technical and organizational measures with the Controller.
6. The Processor shall support the Controller within the scope of its possibilities in fulfilling the requests and claims of data subjects pursuant to Chapter III of the GDPR and in complying with the obligations set forth in Articles 32 to 36 of the GDPR.
7. If a data subject asserts rights, such as the right to information, correction or deletion of their data, directly against the Processor, the Processor shall immediately forward this request to the Controller and await the Controller instructions. The Processor will not contact the data subject without corresponding individual instructions.
8. The Processor warrants that the employees involved in the processing of the Controller's data and other persons working for the Processor are prohibited from processing the data outside the scope of the instruction. Furthermore, the Processor warrants that the persons authorized to process the personal data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality. The confidentiality/confidentiality obligation shall continue to exist after termination of the order.
9. The Processor shall inform the Controller without undue delay if it becomes aware of any violations of the Controller's personal data protection.
10. The Processor shall take the necessary measures to secure the data and to mitigate any possible adverse consequences for the data subjects and shall consult with the Controller on this without delay.
11. The Processor shall name the contact person for the Controller for data protection issues arising within the scope of the contract.
12. The Processor warrants to comply with its obligations under Article 32(1)(d) of the GDPR to implement a procedure for the regular review of the effectiveness of the technical and organizational measures to ensure the security of the Processing.
13. The Processor shall correct or delete the data that is the subject of the contract if the Controller instructs it to do so and this is covered by the scope of the instructions. If a deletion in compliance with data protection or a corresponding restriction of data processing is not possible, the Processor shall undertake the destruction of data carriers and other materi-

als in compliance with data protection on the basis of an individual order by the Controller or shall return these data carriers to the Controller, unless already agreed in the contract.

14. In special cases to be determined by the Controller, storage or handover shall take place; remuneration and protective measures for this shall be agreed separately, unless already agreed in the contract.
15. Data, data carriers and all other materials must either be returned or completely and irrevocably deleted at the request of the Controller after the end of the order, unless a statutory retention period precludes this. This shall also apply to copies of the Controller data made by the Processor, such as data backups, but not to the Processor's documentation which serves as proof that the Controller data has been processed in accordance with the order and properly. Such documentation shall be retained by the Processor for a period of two years from completion and shall be handed over to the Controller upon request for the purpose of documentation. This shall not prevent the Processor from retaining documentation for longer under the statutory conditions, up to a maximum of three months after expiry of the statutory limitation period for any claims of the Controller arising from the contractual relationship.
16. At the request of the Controller, the Processor shall confirm the deletion to the Controller in writing.
17. If additional costs arise due to deviating specifications for the release or deletion of the data, these shall be borne by the Controller.
18. In the event of a claim against the Principal by a data subject with regard to any claims under Art. 82 GDPR, § 3 (4) shall apply accordingly.
19. The defense of the right of retention within the meaning of § 273 BGB is excluded with regard to the data processed in the order.

5 Inspection options

1. Upon request, the Processor shall prove to the Controller compliance with the obligations set forth in this Agreement by appropriate means.
2. Should inspections by the Controller or an auditor commissioned by the Controller be necessary in individual cases, such inspections shall be conducted during regular business hours, without disrupting operations, upon prior notice and with reasonable advance notification. The Processor may make such inspections conditional upon prior notice with reasonable lead time and upon the signing of a non-disclosure agreement concerning the data of other customers and the technical and organizational measures in place. Prior notice shall exceptionally not be required where such notice would defeat the purpose of the inspection. Should the auditor commissioned by the Controller be in a competitive

relationship with the Processor, the Processor shall have a right to object to that auditor.

3. Should a data protection supervisory authority or any other sovereign supervisory authority of the Controller carry out an inspection, (2) shall apply accordingly in principle. It is not necessary to sign a confidentiality agreement if this supervisory authority is subject to professional or statutory confidentiality where a violation is punishable under the German Criminal Code.
4. The Processor processes data through mobile working or in private homes (home office). The Processor shall also ensure the measures pursuant to Article 32 of the GDPR ("TOM") in this case.

6 Subprocessors

1. The Processor engages suitable subprocessors for data processing under this contract. A current list of subprocessors is provided as an **annex** to this contract.
2. The Processor may commission further and/or other subprocessors, provided that the Processor informs the Controller thereof in text form and the Controller has not objected to the intended commissioning at least in text form within a period of four weeks from receipt of the information. If no objection to the intended assignment is raised within the aforementioned period, this shall be deemed to be the Controller's consent. If the Controller raises an objection, the Processor may, at its own discretion, provide the services without the intended commissioning. If it is not reasonable or possible for the Processor to provide the Services without the intended assignment, the Processor shall notify the Controller thereof without undue delay. In this case, the Controller may terminate the framework agreement between the Parties in writing within a period of two weeks from receipt of the Processor's notification.
3. The Processor shall ensure that only those subprocessors are engaged who provide sufficient guarantees that appropriate technical and organizational measures are in place so that the processing of the Controller's personal data is carried out in accordance with the requirements of the GDPR and applicable national data protection laws and the protection of the rights of the data subjects is ensured. The Processor shall carefully select a subprocessor, paying particular attention to the suitability of the technical and organizational measures taken by the sub-processor, and shall regularly review the sub-processor's compliance with the legal and contractual data protection requirements.
4. The Processor shall ensure that the agreement reached between it and the subprocessor is governed by a written contract that contains at least the same data protection obligations for the subprocessor as those set forth in this contract for the Processor. To the extent applicable to the Controller, the Processor shall furthermore contractually agree

with the subprocessor to observe the statutory, professional, or other special confidentiality and secrecy obligations applicable to the Controller, in particular those arising from sector-specific provisions governing professional secrecy (e.g. Section 43e BRAO).

5. The disclosure of personal data to a subprocessor is only permitted if the Processor has satisfied itself in a documented manner that the subprocessor fully complies with its obligations and that a contract has been concluded in accordance with Art. 28 GDPR.
6. The Processor shall remain responsible to the Controller for compliance with the obligations under this Agreement and shall be liable to the Controller if the subprocessor fails to comply with its data protection obligations.

7 Transfer to third countries

Data processing shall take place exclusively within the territory of the Federal Republic of Germany, a member state of the European Union or in another state party to the Agreement on the European Economic Area. Any transfer of processing to another country ("third country"), including through the involvement of any subprocessors, requires the prior consent of the Controller and may only take place if the special requirements for data exports to third countries (esp. Art. 44 et seq. GDPR) are met.

8 Liability

The Controller and the Processor shall be liable to data subjects in accordance with the statutory provisions of Art. 82 GDPR. This shall not affect the Processor's liability to the Controller for breach of obligations under this Agreement or the Framework Agreement.

9 Running time

1. This Data Processing Agreement shall automatically enter into force on the date of signing of the framework agreement and shall remain effective until the termination of the framework agreement. If desired, it can also be additionally signed by both parties.
2. If the framework agreement can be terminated by ordinary notice, the provisions on ordinary termination shall apply accordingly. In case of doubt, termination of the framework agreement shall also be deemed termination of this agreement and termination of this agreement shall be deemed termination of the framework agreement.

3. The Controller is entitled to extraordinary termination of this contract for good cause at any time. Good cause shall be deemed to exist if the Processor fails to comply with its obligations under this contract, intentionally or grossly negligently violates provisions of the GDPR or is unable or unwilling to carry out an instruction of the Controller. In the case of simple - i.e. neither intentional nor grossly negligent - violations, the Controller shall first set the Processor a reasonable deadline within which the Processor can remedy the violation. If this deadline expires without result, the Controller shall then be entitled to extraordinary termination.

10 Information obligations, written form clause, choice of law

1. If the Controller's data at the Processor is endangered by attachment or seizure, by insolvency or composition proceedings or by other events or measures of third parties, the Processor shall inform the Controller thereof without undue delay. The Processor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lies exclusively with the Controller as the "responsible party" within the meaning of the General Data Protection Regulation.
2. Amendments and supplements to this Annex and all of its components - including any warranties of the Processor - shall require a written agreement, which may also be in an electronic format (text form), and the express indication that it is an amendment or supplement to these Terms and Conditions. This shall also apply to the waiver of this formal requirement.
3. In the event of any contradictions, the provisions of this Annex on data protection shall take precedence over the provisions of the Agreement. Should individual parts of this Annex be invalid, this shall not affect the validity of the rest of the Annex.
4. Applicable law and place of jurisdiction are governed by the main contract.

Annexes

- Technical & Organizational Measures (TOMs)
- List of Subprocessors