Data Processing Agreement

The version of this document in German is the definitive legal version. The translation into English is available for your ease of reference only.

SECTION I

1. Purpose and scope

1.1. These Standard Contractual Clauses (hereinafter the "Clauses") are intended to ensure compliance with Article 28(3) and (4) 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, on the free movement of such data, and repealing Directive 95/46/EC.

1.2. The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

1.3. These Clauses apply to the processing of personal data as specified in Annex II.

1.4. Annexes I to IV form an integral part of the Clauses.

1.5. These Clauses are without prejudice to the obligations to which the controller is subject under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

1.6. These Clauses alone do not ensure compliance with obligations related to international data transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

2. Non-modification of the Clauses

2.1. The parties undertake not to modify the Clauses, except for the purpose of adding or updating the information set out in the Annexes.

2.2. This does not prevent the parties from incorporating the Standard Contractual Clauses laid down in these Clauses into a broader contract and from adding other clauses or additional safeguards, provided that these do not directly or indirectly contradict the Clauses or prejudice the fundamental rights or freedoms of data subjects.

3. Interpretation

3.1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, those terms shall have the same meaning as in the respective Regulation.

3.2. These Clauses shall be interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

3.3. These Clauses shall not be interpreted in a way that conflicts with the rights and obligations provided for in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, or that prejudices the fundamental rights or freedoms of data subjects.

4. Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements existing between the parties at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

5. Docking clause

5.1. An entity that is not a party to these Clauses may, with the agreement of all parties, accede to these Clauses at any time as a controller or as a processor by completing the Annexes and signing Annex I.

5.2. Once the Annexes referred to in 5.1 have been completed and signed, the acceding entity shall be treated as a party to these Clauses and shall have the rights and obligations of a controller or processor, in accordance with its designation in Annex I.

5.3. The acceding entity shall have no rights or obligations arising under these Clauses for the period prior to becoming a party.

SECTION II – OBLIGATIONS OF THE PARTIES

6. Description of processing

The details of the processing operations, in particular the categories of personal data and the purposes for which the personal data are processed on behalf of the controller, are specified in Annex II.

7. Obligations of the parties

7.1. Instructions

7.1.1. The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The controller may give further instructions at any time throughout the duration of the processing of personal data. Such instructions shall always be documented.

7.1.2. The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679, Regulation (EU) 2018/1725, or applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose or purposes set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

The processor shall process the data only for the duration specified in Annex II.

7.4. Security of processing

7.4.1. The processor shall implement at least the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the data (hereinafter a "personal data breach"). In assessing the appropriate level of security, the parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing, and the risks for the data subjects.

7.4.2. The processor shall grant members of its personnel access to the personal data undergoing processing only to the extent strictly necessary for implementing, managing and monitoring the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

Where the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "Sensitive Data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance with the Clauses

7.6.1. The parties shall be able to demonstrate compliance with these Clauses.

7.6.2. The processor shall deal promptly and adequately with inquiries from the controller relating to the processing of data in accordance with these Clauses.

7.6.3. The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations laid down in these Clauses and stemming directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the controller may take into account relevant certifications held by the processor.

7.6.4. The controller may choose to conduct the audit itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

7.6.5. The parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority or authorities upon request.

7.7. Use of sub-processors

7.7.1. The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to object to such changes before the relevant

sub-processor(s) are engaged. The processor shall provide the controller with the information necessary to enable the controller to exercise its right to object.

7.7.2. Where the processor engages a sub-processor to carry out specific processing activities (on behalf of the controller), such engagement shall be governed by a contract that imposes on the sub-processor, in substance, the same data protection obligations as those imposed on the processor under these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject under these Clauses and under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

7.7.3. At the controller's request, the processor shall provide the controller with a copy of such a sub-processing agreement and any subsequent amendments thereto. To the extent necessary to protect business secrets or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing a copy.

7.7.4. The processor shall remain fully liable to the controller for the performance of the sub-processor's obligations in accordance with the contract concluded between the processor and the sub-processor. The processor shall notify the controller if the sub-processor fails to fulfil its contractual obligations.

7.7.5. The processor shall agree with the sub-processor a third-party beneficiary clause according to which, in the event the processor has factually disappeared, ceased to exist in law or has become insolvent, the controller shall have the right to terminate the sub-processing contract and to instruct the sub-processor to erase or return the personal data.

7.8. International data transfers

7.8.1. Any transfer of data by the processor to a third country or an international organisation shall be carried out only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject, and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

7.8.2. The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7 for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor may ensure compliance with Chapter V of Regulation (EU) 2016/679 by using Standard Contractual Clauses adopted by the Commission pursuant to Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those Standard Contractual Clauses are met.

8. Assistance to the controller

8.1. The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to that request itself unless authorised to do so by the controller.

8.2. Taking into account the nature of the processing, the processor shall assist the controller in fulfilling the controller's obligation to respond to requests from data subjects to exercise their rights. In fulfilling its obligations under Clauses 8.1 and 8.2, the processor shall comply with the controller's instructions.

8.3. In addition to the processor's obligation to assist the controller pursuant to Clause 8.2, the processor shall furthermore, taking into account the nature of the data processing and the information available to it, assist the controller in ensuring compliance with the following obligations:

8.3.1. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (hereinafter a "data protection impact assessment") where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

8.3.2. the obligation to consult the competent supervisory authority or authorities prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

8.3.3. the obligation to ensure that personal data are accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing are inaccurate or have become outdated;

8.3.4. the obligations under Article 32 of Regulation (EU) 2016/679.

8.4. The parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

9. Notification of personal data breaches

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or, where applicable, Articles 34 and 35 of Regulation (EU) 2018/1725, taking into account the nature of processing and the information available to the processor.

9.1. Breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

9.1.1. in notifying the personal data breach to the competent supervisory authority or authorities, without undue delay after the controller has become aware of it, where relevant (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

9.1.2. in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

9.1.2.1. the nature of the personal data including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

9.1.2.2. the likely consequences of the personal data breach;

9.1.2.3. the measures taken or proposed by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay;

in complying with the obligation pursuant to Article 34 of Regulation (EU) 2016/679 to communicate the personal data breach to the data subject, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2. Breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after becoming aware of the breach. Such notification shall contain, at least:

9.2.1. a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects concerned and the approximate number of data records concerned);

9.2.2. the contact details of a contact point from which more information concerning the personal data breach can be obtained;

9.2.3. its likely consequences and the measures taken or proposed to address the personal data breach, including measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The parties shall set out in Annex III any other elements the processor shall provide when assisting the controller in compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

10. Non-compliance with the Clauses and termination

10.1. Without prejudice to the provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, where the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller if, for any reason, it is unable to comply with these Clauses.

10.2. The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

10.2.1. the controller has suspended the processing of personal data by the processor pursuant to Clause 10.1 and compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

10.2.2. the processor is in substantial or persistent breach of these Clauses or of its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

10.2.3. the processor fails to comply with a binding decision of a competent court or the competent supervisory authority or authorities regarding its obligations pursuant to these Clauses, Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

10.3. The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1.2, the controller insists on compliance with those instructions.

10.4. Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or return all the personal data to the controller and delete existing copies, unless Union or Member State law requires storage of the personal data. Until the data are deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I – LIST OF PARTIES

1. Controller(s)

The controller is the respective customer; the name, address and contact details result from the data stored as part of the registration or contractual relationship.

2. Processor

Evolo Software GmbH, Görrestraße 48, 80797 Munich. Contact person: info@pictomento.com

Data protection contact of the processor

For inquiries regarding data processing, data protection and support in data protection-related matters of the controller, the processor may be contacted via the designated contact address:

Evolo Software GmbH
Görrestraße 48
80797 Munich
E-mail: info@pictomento.com

Data Protection Officer of the Processor

The Processor has appointed a Data Protection Officer.
The Data Protection Officer can be contacted at:

Evolo Software GmbH
Data Protection Officer
Görrestraße 48
80797 Munich
Germany
E-mail: info@pictomento.com

ANNEX II – DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data are processed
Users, visitors, photographers, customers of the photographers, depicted persons (guests).

Categories of personal data processed
Name, e-mail address, user behaviour, IP address, log data, authentication data, profile data, billing data, gallery metadata, media and content data (photos/videos), EXIF metadata, facial recognition data.

Sensitive data processed and applied restrictions or safeguards that fully take into account the nature of the data and the risks involved

Sensitive data processed
Biometric data in the form of facial recognition data, embeddings and derived matching information.

Applied restrictions or safeguards
PictoMento may provide an optional function for the face-based assignment of content. If this function is activated by the customer for a specific gallery, invited persons may be shown, as a priority, content in which they are likely depicted.

Activation of the function takes place exclusively at the customer's instruction for the respective gallery. By activating the function, the customer confirms that there is an appropriate legal basis for the associated processing and that, where required, valid consents or other necessary legal permissions are in place.

The customer is responsible for taking into account declarations of data subjects, in particular withdrawals of consent or objections to processing, and for implementing or arranging without delay any measures resulting from such declarations vis-à-vis the processor.

If the function is deactivated or the underlying gallery is deleted, the associated facial recognition data shall be deleted in accordance with the processor's technical and organisational processes, unless statutory retention obligations prevent this.

Nature of the processing
Collection, storage, retrieval, assignment, prioritisation of the display of content, transmission, deletion, facial recognition.

Purpose(s) for which the personal data are processed on behalf of the controller
Provision of SaaS software for the creation, administration and sharing of online galleries for photographers, including the optional function of showing invited persons, as a priority, content in which they are depicted.

Duration of the processing
For the duration of the main contract.

Access to content and support cases

The processor shall process personal data only to the extent necessary for the provision, technical operation, protection, maintenance and contractual performance of the service.

There shall be no routine substantive access to photo, video or gallery data stored by the controller. Where access is necessary in individual cases for error analysis, troubleshooting, prevention of

misuse, security review or compliance with an instruction from the controller, such access shall be limited to authorised persons and to the extent necessary to achieve the relevant purpose.

Where technically provided for and reasonable, such activities shall be documented internally in a traceable manner. The processor shall ensure through organisational and technical measures that support activities involving possible access to content remain limited to exceptional cases.

Handling requests from data subjects

Where data subjects contact the processor directly, the processor shall forward such requests to the controller without undue delay, unless independent handling is legally required. The processor shall support the controller in handling such requests within the framework of contractual and legal obligations.

Processing by (sub-)processors
Subject matter of the (sub-)processing: Provision of cloud infrastructure, payment processing and accounting services.
Nature of the (sub-)processing: Payment (Mollie), billing (sevDesk), storing (Storj)
Until the end of the contract

ANNEX III – TECHNICAL AND ORGANISATIONAL MEASURES, INCLUDING TO ENSURE THE SECURITY OF THE DATA

Measures for the pseudonymisation and encryption of personal data
Encryption in transit (TLS/SSL), encryption of sensitive data fields and password hashing in accordance with the state of the art (Argon2).

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
Use of encryption, monitoring and alerting mechanisms, role-based access concepts and regular data backups.

Measures for ensuring the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident
Regular data backups; procedures for restoring data and systems are reviewed or test-verified at appropriate intervals in order to enable restoration within an appropriate period of time.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
Regular internal review of the technical setup, ongoing monitoring of security-relevant events and needs-based adaptation of existing protective measures.

Measures for user identification and authorisation

Access to production systems is assigned on a personal basis and managed according to a role-based authorisation concept. Administrative or otherwise highly privileged access is additionally protected, where technically provided for, by a second authentication factor or comparable enhanced authentication. Authorisations are reviewed at appropriate intervals and adjusted or withdrawn without delay when no longer required.

Measures for the protection of data during transmission
Encryption in transit (TLS/SSL) for publicly accessible endpoints; internal system communication takes place within a technically segregated network or equivalent protected infrastructure.

Measures for the protection of data during storage
Encryption of sensitive data fields, secure secret and key management, and password hashing in accordance with the state of the art.

Measures for ensuring the physical security of locations where personal data are processed
Processing takes place in technically secured operating environments. To the extent that external data centres or infrastructure service providers are used, their physical security is ensured within the responsibility of the respective providers according to market-standard security standards.

Measures for ensuring event logging
Monitoring and alerting via Grafana.

Measures for ensuring system configuration, including default configuration
Security-relevant system events and access to administrative functions are logged, where technically provided for, and evaluated to detect disruptions, misconfigurations, unauthorised access or misuse.

Measures for internal IT and IT security governance and management
Internal policies for the management of access, roles, secrets and security-relevant configurations; review and further development of technical and organisational measures as needed.

Measures for certification/quality assurance of processes and products
Where available, audit reports, security evidence or other suitable documentation are used for internal quality assurance. No specific certification is guaranteed hereby.

Measures for ensuring data minimisation
Only such personal data are processed as are necessary for the provision, security, maintenance and performance of the service.

Measures for ensuring data quality
Plausibility checks, technical validations and event-driven correction processes support the accuracy and up-to-dateness of the processed data.

Measures for ensuring limited data retention
Automated or organisationally controlled deletion routines and restriction of data collection and storage to what is necessary for the respective processing purpose.

Measures for ensuring accountability
Internal documentation of technical and organisational measures, regular review of security concepts and documented processes for evaluating and adapting protective measures.

Measures for enabling data portability and ensuring erasure
Provision in a structured format where technically provided for or contractually owed, and implementation of deletion processes in accordance with contractual, technical and statutory requirements.

Description of the specific technical and organisational measures to be taken by the (sub-)processor to assist the controller

Conclusion of data processing agreements with relevant service providers, appropriate review of their technical and organisational measures, and regular review of the service providers involved.

Further development of the technical and organisational measures

The processor is entitled to further develop, adapt or replace the technical and organisational measures described in this Annex with equivalent measures, provided that the overall level of protection owed is not reduced. The processor shall inform the controller, upon request or in another appropriate manner, of significant changes relevant to the security of the processing.

SUPPLEMENTARY PROCEDURAL RULES

Conduct of audits and provision of evidence

The exercise of audit and evidence rights by the controller shall take into account the statutory requirements, the confidentiality interests of other customers, the integrity of the processor's systems and the processor's operational processes.

Where appropriate, compliance with data protection obligations shall first be demonstrated by providing documents, self-assessments, descriptions of technical and organisational measures, certificates, audit reports or comparable suitable evidence.

On-site audits shall be considered in particular where equivalent evidence cannot be provided in another way or is insufficient, or where there are concrete indications of significant breaches of duty. Such audits shall be announced with reasonable notice, carried out during normal business hours and limited to the extent necessary. As a rule, no more than one cause-free on-site audit per calendar year shall take place.

Return and deletion after termination of the contract

After termination of the contractual relationship, the return or deletion of the personal data processed on behalf of the controller shall take place in accordance with the controller's instruction and within the technical possibilities of the service provided, unless statutory retention obligations or other legally permissible reasons for limited temporary retention apply.

Where return is envisaged, the processor shall make the data available via an appropriately secured procedure in a common structured format. If access credentials are required for retrieval, these shall be transmitted separately or provided by another suitable means.

Upon request, the processor shall confirm the deletion carried out in an appropriate form. Documentation serving as proof of proper and contract-compliant processing may be retained beyond the end of the contract to the extent permitted by law.

ANNEX IV – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Name: Storj Labs Inc.
Address: 1870 The Exchange SE Ste 220 PMB 75268, Atlanta, GA 30339-2171, USA
Name, role and contact details of the contact person: legal@storj.io
Description of processing: Object storage for photos, profile pictures, and database and log backups.

Name: Mollie B.V.; Address: Keizersgracht 126, 1015 CW Amsterdam, Netherlands; Description of processing: Payment service provider for the processing of payments.
Name: sevDesk GmbH; Address: Im Unteren Angel 1, 77652 Offenburg, Germany; Description of processing: Accounting and invoicing tool.