

DATA PROCESSING AGREEMENT

Eyevinn Open Source Cloud, standard Data Processing Agreement, version 3.1, dated 23 October 2026

This Data Processing Agreement (the “DPA”) sets out the terms under which Eyevinn Technology AB processes personal data on behalf of its customers in the Open Source Cloud services, as required by Article 28(3) of the GDPR. It is one standard agreement, offered on the same terms to every customer. The parties to a given instance of this DPA are identified on its Cover Sheet (Annex 4).

PARTIES

Processor:

Eyevinn Technology AB, a company registered in Sweden
Organisation number: 556919-9952
Address: Vasagatan 52, 111 20 Stockholm, Sweden
Contact for data protection matters: privacy@eyevinn.se
(operator of the Open Source Cloud platform, www.osaas.io)
 (“**Eyevinn**”)

Controller:

Legal name: _____
Organisation / registration number: _____
Address: _____
OSC workspace (tenant) identifier(s): _____
Contact for data protection matters (name, email): _____
(the “**Customer**”)

Eyevinn and the Customer are each a “**Party**” and together the “**Parties**”. Where a completed Cover Sheet (Annex 4) is attached, the details on the Cover Sheet complete the Controller fields above.

1. BACKGROUND AND SCOPE

1.1. Eyevinn provides the Open Source Cloud services (the “**Services**”) to the Customer under the Eyevinn Open Source Cloud Terms of Service published at www.osaas.io/terms, together with the documents those Terms incorporate (the “**Principal Agreement**”).

1.2. When the Customer uses the Services to process personal data, the Customer is the controller and Eyevinn is its processor within the meaning of Article 4 of the GDPR. This DPA governs that processing.

1.3. This DPA does not cover personal data for which Eyevinn is itself the controller: account and sign-in data, billing and payment data, support correspondence, and platform-operations records, including the operational audit log of calls made through the OSC MCP server. That processing is described in Eyevinn’s Privacy Policy at www.osaas.io/privacy.

2. DEFINITIONS

- 2.1. **“GDPR”** means Regulation (EU) 2016/679. **“Applicable Data Protection Law”** means the GDPR and any EU or Member State law supplementing it that applies to the processing, including in Sweden the Act (2018:218) containing supplementary provisions to the GDPR.
- 2.2. **“Personal data”, “processing”, “controller”, “processor”, “data subject”, “personal data breach” and “supervisory authority”** have the meanings given in Article 4 of the GDPR.
- 2.3. **“Customer Personal Data”** means personal data that Eyevinn processes on behalf of the Customer in providing the Services, including personal data that the Customer or its own end users store in, transmit through or generate with the Customer’s applications and service instances on the Services.
- 2.4. **“Sub-processor”** means a processor engaged by Eyevinn, or by another Sub-processor, to process Customer Personal Data.
- 2.5. **“Sub-processor List”** means the list of Sub-processors published at www.osaas.io/subprocessors, as updated in accordance with clause 7.
- 2.6. **“SCCs”** means the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
- 2.7. **“AI Features”** means the two Open Source Cloud features through which Eyevinn, on its own account, sends content to a third-party AI model provider: (a) the AI assistant in the OSC web console, and (b) the ask-osc-architect tool on the OSC MCP server.

3. DETAILS OF THE PROCESSING

- 3.1. The subject matter, duration, nature and purpose of the processing, the types of personal data and the categories of data subjects are set out in Annex 1.
- 3.2. Open Source Cloud is a general-purpose platform. The Customer decides which personal data it processes on the Services and is responsible for having a lawful basis for that processing.

4. DOCUMENTED INSTRUCTIONS (Article 28(3)(a))

- 4.1. Eyevinn shall process Customer Personal Data only on documented instructions from the Customer, including with regard to transfers to a third country, unless required to do so by EU or Member State law to which Eyevinn is subject. In that case Eyevinn shall inform the Customer of that legal requirement before processing, unless that law prohibits this on important grounds of public interest.
- 4.2. The Customer’s documented instructions are this DPA, the Principal Agreement, and the Customer’s own use and configuration of the Services, including the service instances it creates, the features it enables, and the requests it or its authorised users make to the AI Features. Further instructions must be given in writing, including by email to privacy@eyeveinn.se.
- 4.3. Eyevinn shall immediately inform the Customer if, in its opinion, an instruction infringes the GDPR or other Applicable Data Protection Law.

5. CONFIDENTIALITY (Article 28(3)(b))

- 5.1. Eyevinn shall ensure that persons authorised to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.2. Eyevinn shall limit access to Customer Personal Data to personnel who need it to provide, operate, support or secure the Services.

6. SECURITY (Article 28(3)(c) and Article 32)

6.1. Eyevinn shall implement and maintain the technical and organisational measures described in Annex 2, which are designed to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing.

6.2. Eyevinn may update the measures in Annex 2, provided that the overall level of security is not reduced.

6.3. The Customer is responsible for the security of what it builds and runs on the Services, including its application code, the configuration of its service instances, the credentials and access it grants, and any encryption it applies at application level.

7. SUB-PROCESSORS (Article 28(2), 28(3)(d) and 28(4))

7.1. **General authorisation.** The Customer gives Eyevinn general written authorisation to engage the Sub-processors on the Sub-processor List. Annex 3 records the Sub-processors as they stood on the date of this DPA.

7.2. **Notice of changes.** Eyevinn shall inform the Customer at least 30 calendar days before adding a new Sub-processor, or replacing one in a way that introduces a new international transfer or a new category of processing. Notice is given by updating the Sub-processor List and by email to the contact for data protection matters named on the Cover Sheet or, if none is named, to the account contact on record. A change of role among Sub-processors already listed, where no new international transfer and no new category of processing arises, is published on the Sub-processor List without advance notice.

7.3. **Right to object.** The Customer may object to a new or replacing Sub-processor on reasonable data protection grounds within 30 days of the notice. The Parties shall then discuss the objection in good faith. If it is not resolved, the Customer may terminate the affected Services without penalty. This right applies whether or not the Customer has signed this DPA separately.

7.4. **Optional features.** Some Sub-processors are engaged only for an optional feature that is off unless the Customer switches it on, such as CDN acceleration, which Elastx AB provides through Varnish Software AB (Annex 3). Such a Sub-processor is listed on the Sub-processor List and is named, with a link to that list, on the screen where the feature is enabled, before it is enabled. By enabling the feature, the Customer authorises that Sub-processor for the content and personal data processed through that feature, and no 30-day advance notice is given for it. If the Customer does not enable the feature, that Sub-processor processes no Customer Personal Data. The Customer may withdraw the authorisation at any time by disabling the feature. If Eyevinn later adds or replaces a Sub-processor for an optional feature the Customer has already enabled, clauses 7.2 and 7.3 apply.

7.5. **Flow-down and liability.** Eyevinn shall engage each Sub-processor it engages directly by a written contract imposing data protection obligations that provide sufficient guarantees to implement appropriate technical and organisational measures, so that the processing meets the requirements of the GDPR. Where a Sub-processor engages another processor for the Services, Eyevinn shall require it to impose the same data protection obligations on that processor by written contract (Article 28(4)). Eyevinn remains fully liable to the Customer for the performance of each Sub-processor's obligations.

7.6. **Providers the Customer engages itself.** Where the Customer runs a service, or uses a platform feature, that calls a third party with credentials the Customer supplies (for example an AI provider API key configured for Agent

Tasks, Agentic SDLC or a catalogue service), or connects its own AI client to the OSC MCP server, that third party is not a Sub-processor of Eyevinn. The Customer engages it under the Customer's own agreement with it, and the Customer, not Eyevinn, is responsible for any transfer of personal data to it. Eyevinn publishes the services and features known to call an AI provider at www.osaas.io/third-party-calls.

8. ASSISTANCE WITH DATA SUBJECT RIGHTS (Article 28(3)(e))

8.1. Taking into account the nature of the processing, Eyevinn shall assist the Customer by appropriate technical and organisational measures, insofar as this is possible, in fulfilling its obligation to respond to requests from data subjects exercising their rights under Chapter III of the GDPR.

8.2. The Customer has direct administrative access to the data it stores on the Services (its databases, object storage, configuration and applications) and can ordinarily answer such requests itself. Eyevinn's assistance applies where the request cannot reasonably be fulfilled with that access.

8.3. If a data subject contacts Eyevinn directly about Customer Personal Data, Eyevinn shall forward the request to the Customer without undue delay and shall not respond to it except on the Customer's documented instructions or where required by law.

9. ASSISTANCE WITH ARTICLES 32 TO 36; PERSONAL DATA BREACHES (Article 28(3)(f))

9.1. Taking into account the nature of the processing and the information available to it, Eyevinn shall assist the Customer in ensuring compliance with Articles 32 to 36 of the GDPR (security of processing, notification of personal data breaches to the supervisory authority and communication to data subjects, data protection impact assessments, and prior consultation).

9.2. **Breach notification.** Eyevinn shall notify the Customer of a personal data breach affecting Customer Personal Data without undue delay and in any event within 48 hours after becoming aware of it. Notice is given to the contact for data protection matters named on the Cover Sheet, or if none is named, to the account contact on record.

9.3. The notification shall describe, to the extent known: the nature of the breach, including where possible the categories and approximate number of data subjects and of personal data records concerned; the likely consequences; and the measures taken or proposed to address the breach and mitigate its effects. Where not all information is available at once, Eyevinn shall provide it in phases without undue further delay.

9.4. Eyevinn shall document each personal data breach affecting Customer Personal Data and shall not notify the supervisory authority or data subjects on the Customer's behalf unless the Customer instructs it to or the law requires it.

10. DELETION OR RETURN AT THE END OF THE SERVICES (Article 28(3)(g))

10.1. During the term of the Services the Customer can export its data at any time using standard, open-format mechanisms, including database dumps for its databases and the S3-compatible API for its object storage.

10.2. When the Services end, Eyevinn shall, at the Customer's choice, delete or return all Customer Personal Data, and delete existing copies, unless EU or Member State law requires storage. The Customer states its choice in writing before the account is closed. If it states no choice, Eyevinn shall delete.

10.3. Eyevinn shall delete Customer Personal Data from the production systems within 90 days of the closure of the Customer's account. Scheduled backups that the Customer has set up for its database instances are stored in the

Customer's own object storage instance on the Services (Annex 2, section B.6) and are deleted with it. Eyevinn also keeps backup copies of the platform's own database (Annex 2, section B.6). Each of those copies is deleted 30 days after it is made. Until a copy is deleted, Eyevinn shall not restore or otherwise use from it any Customer Personal Data of a closed account, and if a copy is used to restore the platform, Eyevinn shall delete again any such data that the restore brings back. Eyevinn shall confirm deletion in writing on request.

10.4. Clause 10 prevails over any provision of the Principal Agreement that would allow Eyevinn to keep a copy of Customer Personal Data after termination.

11. TRANSFERS OUTSIDE THE EU/EEA (Chapter V of the GDPR)

11.1. Hosting. The infrastructure on which the Customer's applications, service instances and data are hosted is provided by Elastx AB in region Stockholm, Sweden. Eyevinn's agreement with Elastx AB prohibits any transfer of the data outside the EU/EEA, including remote access for administration, support, maintenance and monitoring. Since 21 October 2026, backup copies of the platform's own database are stored in Elastx AB's backup storage service (The Vault) in Sweden, under the same agreement. Copies made before that date remain with Amazon Web Services in region eu-north-1, Stockholm, Sweden, on the terms stated for it in Annex 3, until they are deleted under clause 10.3.

11.2. The AI Features. When the Customer or its authorised users use an AI Feature, the content of that use is sent to the AI model provider named for the AI Features on the Sub-processor List. That content consists of the prompts and questions submitted and, in the case of the console assistant, the information the assistant retrieves from the Customer's workspace at the user's request in order to answer, for example application and service logs, lists of objects in storage buckets, and responses from the Customer's service instances. Those providers operate from the United States. For these transfers Eyevinn, as data exporter, relies on the SCCs, Module Three (processor to processor). Eyevinn does not rely on the EU-US Data Privacy Framework for these transfers. Eyevinn limits its own storage of conversations with the AI Features to 7 days and pseudonymises user identifiers, and the Customer can switch off conversation storage for its workspace under AI Preferences in the OSC dashboard. The Customer can prevent this transfer of Customer Personal Data by not using the AI Features for matters involving services that hold personal data.

11.3. Ancillary and optional Sub-processors. Any other transfer of Customer Personal Data outside the EU/EEA, including through an optional feature under clause 7.4, takes place only to a Sub-processor on the Sub-processor List, on the safeguard stated for it there.

11.4. New transfers. Eyevinn shall not begin a new transfer of Customer Personal Data outside the EU/EEA except in accordance with clause 7.

12. INFORMATION AND AUDIT (Article 28(3)(h))

12.1. Eyevinn shall make available to the Customer all information necessary to demonstrate compliance with Article 28 of the GDPR and this DPA, and shall allow for and contribute to audits, including inspections, conducted by the Customer or by an auditor mandated by the Customer.

12.2. Eyevinn shall first answer the Customer's request with documentation. Where the Customer reasonably considers this insufficient, an audit or inspection may take place on at least 30 days' written notice (or shorter notice following a personal data breach or where a supervisory authority requires it), during Swedish business hours, no more than once in any 12-month period unless a breach has occurred or a supervisory authority requires otherwise, and by an auditor bound by confidentiality who is not a competitor of Eyevinn. Each Party bears its own costs.

12.3. Eyevinn does not hold an ISO/IEC 27001 certificate of its own. Its hosting provider, Elastx AB, holds an ISO/IEC 27001:2022 certificate for its cloud platform services.

13. LIABILITY, TERM AND PRECEDENCE

13.1. **Liability.** The limitations of liability in the Principal Agreement apply to this DPA. Nothing in this DPA limits liability that cannot be limited under Applicable Data Protection Law, including liability towards data subjects under Article 82 of the GDPR.

13.2. **Term.** This DPA takes effect on the date it is entered into under clause 14 and remains in force for as long as Eyevinn processes Customer Personal Data on behalf of the Customer, including until clause 10 has been completed.

13.3. **Precedence.** As regards Eyevinn's processing of Customer Personal Data as processor, this DPA prevails over the Principal Agreement and the Privacy Policy. Where the SCCs apply, they prevail over this DPA. The Sub-processor List forms part of this DPA through clause 7 and Annex 3.

13.4. **Amendment.** Amendments to this DPA must be in writing. Eyevinn may issue a new version of its standard DPA. Eyevinn shall send the new version by email to the contact for data protection matters named on the Cover Sheet or, if none is named, to the account contact on record, at least 30 days before Eyevinn asks the Customer to accept it. A new version applies to the Customer only once the Customer accepts it under clause 14. Until then the version the Customer last accepted continues to apply. This clause does not apply to updates to Annex 2 under clause 6.2 or to changes to the Sub-processor List under clause 7.

13.5. **Governing law and disputes.** This DPA is governed by the substantive laws of Sweden, excluding its conflict of laws rules. Disputes are resolved as provided in the Principal Agreement (arbitration under the Rules of the Arbitration Institute of the Stockholm Chamber of Commerce).

14. ENTERING INTO THIS DPA

14.1. This DPA may be entered into in either of the following ways:

- (a) by both Parties signing the Cover Sheet (Annex 4) by hand or with an electronic signature service; or
- (b) by electronic acceptance: the Customer returns the completed Cover Sheet, or states in an email sent to privacy@eyeveinn.se by a person authorised to represent the Customer, that it accepts this DPA in the version identified on the Cover Sheet, and Eyevinn confirms the acceptance in writing by email; or
- (c) by acceptance in the Open Source Cloud console: a user with administrator rights for the Customer's workspace completes the Cover Sheet fields on the Data Processing Agreement page and confirms that they are authorised to represent the Customer and accept this DPA in the version shown. Eyevinn records the acceptance (the user, the time, the version and the Cover Sheet details) and sends the completed Cover Sheet and this DPA by email to that user and to the contact for data protection matters. That email is Eyevinn's written confirmation.

14.2. A DPA entered into under clause 14.1(b) or (c) has the same effect as one signed under clause 14.1(a).

14.3. **Incorporation in the Principal Agreement.** This DPA forms part of the Principal Agreement. It applies to Eyevinn's processing of Customer Personal Data from the date the Customer accepted a version of the Principal Agreement that incorporates it, whether or not the Customer has also entered into it under clause 14.1. A Customer that has not completed a Cover Sheet is identified by its account details, and notices to it go to the account contact on record. Completing a Cover Sheet under clause 14.1 adds the Controller details and the Customer's choice under clause 10.2.

ANNEX 1, DETAILS OF THE PROCESSING

A. Subject matter. Provision of the Open Source Cloud services to the Customer: hosting of the Customer's applications and code, and the operation of the open-source service instances (for example databases, object storage and caches) that the Customer creates.

B. Duration. For the term of the Services and thereafter until clause 10 has been completed.

C. Nature of the processing. Storage, hosting, retrieval, transmission, backup, container orchestration, operation of databases and service instances, logging and monitoring necessary to run and secure the Services, and, where the Customer uses them, the AI Features (clause 11.2) and the optional CDN acceleration feature (clause 7.4). Eyevinn performs no profiling, advertising or enrichment on Customer Personal Data and does not use it for its own purposes.

D. Purpose. To provide the Services so that the Customer can run its own applications and services.

E. Categories of data subjects. Determined by the Customer. They may include the Customer's own customers and end users, visitors to the Customer's applications, and the Customer's employees and contractors.

F. Types of personal data. Determined by the Customer. They may include identity and contact data, account and authentication data of the Customer's own end users, order and transaction data, content and files stored by the Customer, and logs and request data (such as IP addresses) generated by the Customer's applications.

G. Special categories and criminal offence data. The Customer shall not process special categories of personal data (Article 9 GDPR) or personal data relating to criminal convictions and offences (Article 10 GDPR) on the Services unless it has first informed Eyevinn in writing and the Parties have agreed any additional measures.

H. Location. As set out in clause 11.

ANNEX 2, TECHNICAL AND ORGANISATIONAL MEASURES

This Annex describes the measures in place on the date of this DPA. Eyevinn describes only measures it has verified, and makes no commitment beyond what is stated here.

A. Hosting provider

A.1. The Services are hosted on infrastructure provided by Elastx AB in region Stockholm, Sweden, under a written data processing agreement. For that hosting, Elastx AB has confirmed that it uses no sub-processors of its own, including for colocation, hardware maintenance, backup and monitoring. Under that agreement Elastx AB may not engage a new sub-processor until it has given Eyevinn written notice and a 30-day objection period has passed without objection, may not transfer the data outside the EU/EEA, including by remote access, and must notify Eyevinn of a personal data breach within 24 hours of becoming aware of it.

A.2. Elastx AB holds ISO/IEC 27001:2022 certificate no. 0095098 for its cloud platform services. This certificate is Elastx AB's and covers its own operations, not Eyevinn's.

A.3. **CDN acceleration.** Elastx AB also resells the optional CDN acceleration feature (clause 7.4) and provides first- and second-line support for it. Varnish Software AB operates the feature as Elastx AB's sub-processor. The terms on which Elastx AB processes personal data for this feature, and the data protection obligations it must impose on Varnish Software AB, are set out in an addendum to Eyevinn's data processing agreement with Elastx AB. On the

date of this DPA that addendum had not been signed. Until it is signed, the location and transfer position for this feature is as stated for Varnish Software AB in Annex 3, and the statements in section A.1 apply to hosting only.

B. Measures operated by Eyevinn

B.1. Encryption in transit. Public endpoints of the Services are served over HTTPS with certificates that are renewed automatically; plain HTTP requests are redirected to HTTPS.

B.2. Tenant separation. The Services run on a Kubernetes platform shared by all customers. Each service instance runs as its own workload with its own credentials and, where it stores data, its own storage volume. Instances of the same service that belong to different customers share a Kubernetes namespace. Separation between customers is enforced by the platform's orchestrator: every operation to create, list, change or delete instances is limited to the workspace named in the caller's signed token, and such tokens cannot be issued without the platform's signing key. The authentication layer in front of an instance's public endpoint checks that the caller holds a valid token; access within the instance is controlled by the instance's own credentials. Eyevinn does not currently apply network-level segmentation (Kubernetes network policies) between customers' workloads, and does not enforce per-customer compute resource limits. A Customer that needs network-level isolation should protect its instances with their own credentials and contact Eyevinn before processing such data on the Services.

B.3. Access control. Access to the Services requires authentication (sign-in with email link, passkey, or a supported identity provider, and personal access tokens for programmatic access). Administrative access to the platform is limited to named Eyevinn personnel who need it.

B.4. Logging. Every call made through the OSC MCP server is written to an operational audit log recording the actor, the tool called, the resource addressed and the outcome. Access to the log is restricted to platform administrators.

B.5. AI Features. Conversations with the AI Features are stored by Eyevinn for at most 7 days, user identifiers are pseudonymised, and the Customer can switch off conversation storage for its workspace. The AI model providers do not use this content to train their models under their commercial API terms.

B.6. Backups. Where the Customer has enabled scheduled backups of a database instance, the backups are stored in a bucket in the Customer's own MinIO object storage instance on the Services, on the Elastx AB infrastructure in region Stockholm, Sweden, and are retained for the number of days the Customer sets for the backup schedule. Separately, Eyevinn backs up the platform's own database, which holds the records Eyevinn keeps to operate the Services, such as accounts, workspaces and the configuration of service instances. These backups are taken at regular intervals. Since 21 October 2026 they are stored in Elastx AB's backup storage service The Vault in Sweden, which is covered by Eyevinn's data processing agreement with Elastx AB (section A.1). That storage is immutable, and the backup job can write copies but cannot delete them. Each copy is kept for 30 days and then deleted (clause 10.3). Copies made before 21 October 2026 are stored in Eyevinn's own Amazon Web Services account in region eu-north-1, Stockholm, Sweden (Annex 3). No new copies are made there, and each remaining copy is deleted 30 days after it was made, the last of them by about 20 November 2026.

B.7. Encryption at rest. Elastx AB has stated to Eyevinn that all storage on its cloud platform is encrypted at rest. Eyevinn has not verified this independently and applies no encryption at rest of its own, so this DPA contains no commitment to encryption at rest of the Customer's databases and object storage. A Customer that needs it can encrypt data at application level (clause 6.3).

B.8. Incident handling. Eyevinn handles security incidents under a documented procedure, including notification to the Customer under clause 9.2.

C. Organisational measures

C.1. Personnel with access to Customer Personal Data are bound by confidentiality (clause 5).

C.2. Sub-processors are engaged only under written agreements meeting clause 7.5.

C.3. Eyevinn maintains an information security management system aligned with ISO/IEC 27001:2022. Eyevinn is not certified.

ANNEX 3, SUB-PROCESSORS

The Sub-processor List at www.osaas.io/subprocessors is the current and governing list (clause 7). The table below records the Sub-processors that process Customer Personal Data as they stood on the date of this DPA.

Sub-processor	Function	When it processes Customer Personal Data	Location	Safeguard
Elastx AB (Sweden)	Compute, storage, networking and managed Kubernetes on which the Services run. Elastx AB also resells, and provides first- and second-line support for, the optional CDN acceleration feature, which Varnish Software AB operates (Annex 2, section A.3). Since 21 October 2026 also storage of backup copies of the platform's own database in The Vault (Annex 2, section B.6)	Always for hosting and platform backups; for CDN acceleration, only if the Customer enables it (clause 7.4)	Region Stockholm, Sweden (EU/EEA)	Hosting: no transfer outside the EU/EEA; data processing agreement in place. CDN acceleration: the addendum to that agreement had not been signed on the date of this DPA (Annex 2, section A.3)
Amazon Web Services	Storage of backup copies of the platform's own database made before 21 October 2026 (Annex 2, section B.6)	Until those copies are deleted, the last of them by about 20 November 2026. No new copies are stored with AWS	Region eu-north-1, Stockholm, Sweden (EU/EEA)	AWS Data Processing Addendum, incorporated in the AWS Service Terms. Under it, AWS does not move the data out of the selected region except as necessary to provide the service or to comply with the law or a binding order of a governmental body; the SCCs 2021/914 incorporated in that addendum (Module Three) apply to any such transfer
OpenAI Ireland Ltd. (data importer under the	AI model provider for the AI Features	Only when the AI Features are used	United States	SCCs 2021/914, Module Three; data processing

Sub-processor	Function	When it processes Customer Personal Data	Location	Safeguard
SCCs: OpenAI OpCo, LLC, United States)				agreement in place
Anthropic, PBC	AI model provider for the AI Features	Only when the AI Features are used	United States	SCCs 2021/914, Module Three; data processing agreement in place
Varnish Software AB (Sweden), engaged by Elastx AB	Content delivery network for endpoints on which the Customer enables CDN acceleration: caches and delivers that content and processes end users' request data at the edge	Only if the Customer enables CDN acceleration (clause 7.4)	Varnish's European edge network. The countries of the edge locations are not yet confirmed and will be stated on the Sub-processor List	Not yet confirmed whether any processing of, or access to, this data takes place outside the EU/EEA; the Sub-processor List will state the safeguard once confirmed. Varnish Software AB processes this data under its agreement with Elastx AB; Eyevinns addendum with Elastx AB covering it had not been signed on the date of this DPA (Annex 2, section A.3)

The Sub-processor List also names providers that act as independent controllers or that process only account and sign-in data for which Eyevinns is controller (for example the payment provider and the optional sign-in identity providers). They are outside this DPA (clause 1.3).

ANNEX 4, COVER SHEET

Data Processing Agreement, Eyevinns Open Source Cloud, version 3.1 dated 23 October 2026

By signing or accepting this Cover Sheet, the Parties enter into the Data Processing Agreement identified above, which is attached and forms part of this Cover Sheet.

Customer (Controller)

Field	Details
Legal name	
Organisation / registration number	
Address	
OSC workspace (tenant) identifier(s)	
Services / applications in scope (optional)	
Contact for data protection matters, including breach notices (name, email)	
Choice at end of Services (clause 10.2): delete / return	

Signatures

For Eyevinn Technology AB (Processor)

Name: Alexander Björneheim

Title: CEO (Verkställande direktör)

Date: _____

Signature: _____

For the Customer (Controller)

Name: _____

Title: _____

Date: _____

Signature: _____

Accepted in the Open Source Cloud console under clause 14.1(c): date _____, user
_____ (completed by the console).

Electronic acceptance under clause 14.1(b) or (c) replaces the signatures above.