Eyk Data Processing Agreement

Version 2.0
2026-11-16

This Data Processing Agreement (“DPA”) forms part of the Eyk Terms and Conditions and governs the processing of Personal Data by Eyk B.V. (“Eyk” or “Processor”) on behalf of the customer that uses the Eyk Service (“Customer” or “Controller”). It replaces the Data Processing Agreement dated 1 April 2023. By accepting the Terms and Conditions, Customer enters into this DPA.

1. Scope and precedence

1.1 This DPA applies to all Processing of Personal Data by Eyk in connection with the Eyk Service, including the platform, server-side tracking and consent management, connectors, data pipelines, the data warehouse, modelling, reporting, the semantic layer, the external API, AI functions, external agent connections, exports, Destinations and customer support.

1.2 For matters concerning the Processing of Personal Data, this DPA prevails over the Terms and Conditions.

1.3 Where Customer enables a connection between the Eyk Service and a third-party tool (including an external AI agent), Eyk’s obligations under this DPA extend to the transfer of data to that tool as instructed, not to the tool’s own Processing.

1.4 Eyk’s privacy contact for questions about this DPA is privacy@eykdata.com.

2. Definitions

2.1 Applicable Data Protection Law means Regulation (EU) 2016/679 (GDPR), the Dutch GDPR Implementation Act (UAVG) and other mandatory privacy law applicable to the Processing.

2.2 Agreement has the meaning given in the Terms and Conditions.

2.3 Customer Data means Personal Data and other data provided by or on behalf of Customer, or generated specifically for Customer, through the Eyk Service.

2.4 Customer Environment means the datasets, tables and storage in which Eyk stores Customer Data for Customer.

2.5 Eyk Service means the SaaS platform and related hosting, tracking, connectors, modelling, reporting, AI and support services provided by Eyk under the Agreement.

2.6 Data Source and Destination mean a third-party system from which the Eyk Service collects data, or to which it sends or gives access to data, that Customer connects in the Eyk platform or by written instruction.

2.7 Subprocessor means a third party engaged by Eyk to Process Personal Data on behalf of Customer, including cloud, hosting, monitoring, authentication and AI model providers where they Process Personal Data. Data Sources and Destinations are not Subprocessors.

2.8 Personal Data Breach has the meaning given in the GDPR.

2.9 Other capitalised terms (Personal Data, Processing, Controller, Processor, Data Subject, Supervisory Authority) have the meaning given in the GDPR.

3. Subject matter, nature, purpose and duration

3.1 Eyk Processes Personal Data solely to provide, secure and support the Eyk Service for Customer and to create aggregated and anonymised data under Clause 14, as described in Schedule 1 and in accordance with Customer’s documented instructions.

3.2 Processing includes collecting, ingesting, transmitting, validating, combining, modelling, pseudonymising, attributing, segmenting, analysing, visualising, storing, activating, exporting, correcting, returning and deleting Personal Data.

3.3 Processing continues for the term of the Agreement and thereafter only for the return and deletion period in Clause 16, backup rotation and any retention required by law.

4. Instructions and self-service configuration

4.1 Eyk Processes Personal Data only on Customer's documented instructions, unless Union or Member State law requires otherwise, in which case Eyk informs Customer of that legal requirement before the Processing, unless that law prohibits this. Documented instructions consist of this DPA, the Agreement, the configuration and settings made by Customer's users in the Eyk platform, and written instructions from Customer's authorised contacts.

4.2 Customer determines the purposes and lawful basis of the Processing and decides which Data Sources, Destinations and AI functions are enabled. Eyk determines the technical manner of delivering the Eyk Service, including its architecture, security measures and development practices, subject to this DPA.

4.3 The Eyk Service is self-service. Customer's users enable and disable Data Sources, Destinations, AI functions and external agent connections in the platform. Enabling a capability is Customer's instruction to Eyk to Process the associated Personal Data for that capability's documented purpose. Any internal approval Customer requires before a user enables a capability is Customer's own responsibility; Eyk is not required to verify it.

4.4 Eyk informs Customer of new Data Sources, Destinations, AI functions and other capabilities through release notes, in-product notices or similar means. A new capability applies to Customer Data only once enabled by Customer, unless it is part of the standard operation of the Eyk Service and does not introduce a new purpose or a new recipient of Personal Data.

4.5 Eyk shall promptly inform Customer if, in Eyk's opinion, an instruction infringes Applicable Data Protection Law, and may suspend the affected Processing until the instruction is confirmed or withdrawn. Fees remain payable during such a suspension.

4.6 Instructions that go beyond the standard functions and documentation of the Eyk Service are performed only if agreed in writing and may be charged at Eyk's then-current rates.

5. Customer obligations

5.1 Customer is responsible for the lawfulness of its instructions, for transparency towards Data Subjects, for obtaining consent or establishing another lawful basis where required (including consent required under ePrivacy rules for cookies, tracking and conversion APIs), and for any Data Protection Impact Assessment it is required to carry out.

5.2 Customer shall not instruct Eyk to Process Personal Data that Customer has no right to provide, and shall not provide special categories of Personal Data, Personal Data relating to criminal convictions and offences or full payment-card data unless agreed in writing.

5.3 Customer manages its own Eyk user accounts and permissions in accordance with least privilege, including which users may enable Data Sources, Destinations, AI functions and external agent connections, and which users and roles may access which data through the Eyk semantic layer.

5.4 Customer configures consent management and the consent conditions that apply to tracking and activation. Eyk applies that configuration and does not override or broaden Customer's consent choices.

5.5 Where Customer enters into this DPA on behalf of affiliates or group brands whose data is Processed in the Customer Environment, Customer acts as their representative, acts and omissions of those affiliates are attributed to Customer, and only Customer may bring claims under this DPA.

6. Confidentiality and personnel

6.1 Eyk ensures that all personnel authorised to Process Customer Data are bound by confidentiality obligations, receive appropriate training and have access only to the extent needed for their duties.

6.2 Access to Customer Data is attributable to individual personnel. Privileged access is controlled and logged. Eyk revokes access without undue delay when it is no longer required.

6.3 Eyk maintains a record of the Processing activities it carries out on behalf of Customer in accordance with Article 30(2) GDPR and makes it available to a Supervisory Authority on request.

7. Processing environment

7.1 Eyk Processes Customer Data in the Customer Environment and through the Subprocessors listed in accordance with Clause 9.

7.2 Customer Data is logically segregated from other customers' data, and Eyk maintains controls designed to prevent cross-customer access, including in AI functions and the external API.

7.3 The Customer Environment, including its backups, is hosted in the EEA. Subprocessors may store or access Personal Data elsewhere only as stated in the Subprocessor list (Clause 10).

8. Security

8.1 Eyk implements appropriate technical and organisational measures to protect Customer Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage or disclosure, taking into account the state of the art, the costs of implementation and the nature of the Processing. The measures in place at the date of this DPA are described in Schedule 2.

8.2 Eyk determines how these measures are implemented. Eyk may change individual measures over time, provided the overall level of protection is not materially reduced, and informs Customer of material changes through release notes, its trust center or similar means.

8.3 Eyk handles vulnerabilities and tests its security and recovery in proportion to the risk, as described in its trust center.

8.4 Eyk applies data protection by design and by default: the Eyk Service ingests the fields required for the functions Customer has enabled, Customer can limit the fields shared from its Data Sources, and Personal Data used outside production is limited to what is needed and protected by access controls and, where practical, masking or pseudonymisation.

9. Subprocessors

9.1 Customer grants Eyk general written authorisation to engage Subprocessors. Eyk lists its Subprocessors, with their service, Processing locations and transfer mechanism, on its published list at www.eykdata.com/trust-center/subprocessors (the "Subprocessor list"), which Eyk keeps current.

9.2 Eyk informs Customer of an intended addition or replacement of a Subprocessor at least 30 days before the new Subprocessor Processes Customer Data, by updating the published list and notifying Customer by email. Where a Subprocessor must be replaced urgently for security or continuity reasons, Eyk notifies Customer as soon as reasonably possible and Customer's objection period under Clause 9.3 runs from that notice.

9.3 Customer may object within 14 days of the notice on reasonable, documented data-protection or security grounds. If Eyk cannot or will not refrain from using the Subprocessor for Customer's Processing, Customer may terminate the affected part of the Eyk Service without penalty before the Subprocessor starts Processing Customer Data. Termination on these terms is Customer's sole remedy for an objection. The export period under Clause 16.3 applies to such a termination.

9.4 Eyk imposes data-protection obligations on each Subprocessor that offer at least the same level of protection as those in this DPA and remains liable to Customer for the Subprocessor's performance of those obligations, subject to Clause 17.

9.5 Data Sources, Destinations and external agents or tools that Customer connects to the Eyk Service are not Subprocessors of Eyk. Their legal role follows from Customer's own relationship with them.

10. International transfers

10.1 Subprocessors may store or access Personal Data outside the EEA only as stated in the Subprocessor list, under a valid transfer mechanism under Chapter V GDPR (an adequacy decision, including the EU-US Data Privacy Framework, or Standard Contractual Clauses with supplementary measures where needed), or on Customer's instruction.

10.2 Where Standard Contractual Clauses apply between Eyk and a Subprocessor, Eyk provides Customer on request with the information reasonably needed for a transfer impact assessment.

11. Personal data breaches

11.1 Eyk notifies Customer without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach affecting Customer Data. Eyk becomes aware when it has established with reasonable certainty that a Personal Data Breach has occurred; a security alert that is still under investigation does not constitute awareness. Where facts are incomplete, Eyk notifies with the information

available and provides updates as the investigation progresses. Eyk sends the notification to the email address Customer registered for its account or to a security contact Customer has designated.

11.2 The notification describes, to the extent known, the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact person.

11.3 Eyk contains the breach, preserves relevant evidence, performs a root-cause analysis and informs Customer of the corrective measures taken.

11.4 Eyk does not notify Data Subjects or Supervisory Authorities on Customer's behalf unless instructed by Customer or required by law. A notification under this Clause is not an admission of liability.

11.5 This Clause does not apply to incidents caused by Customer, its users or the third-party tools and Destinations Customer has connected, although Eyk informs Customer of such incidents where it becomes aware of them. Customer does not publicly name Eyk in connection with a Personal Data Breach without Eyk's prior written approval, unless required by law.

12. Data subject requests and assistance

12.1 Eyk assists Customer, through the functions of the Eyk Service and otherwise with appropriate measures, in responding to Data Subject requests for access, rectification, erasure, restriction, portability and objection. Assistance that goes beyond the standard functions of the Eyk Service may be charged at Eyk's then-current rates.

12.2 Eyk does not respond directly to a Data Subject except on Customer's instruction or where required by law, in which case Eyk informs Customer unless prohibited.

12.3 Taking into account the nature of the Processing and the information available to Eyk, Eyk reasonably assists Customer with Data Protection Impact Assessments, prior consultation with a Supervisory Authority and records of Processing, and provides the information reasonably required to assess server-side tracking, conversion APIs, attribution, segmentation and AI functions. Eyk may charge reasonable costs for assistance that goes beyond the standard documentation and functions of the Eyk Service.

12.4 Eyk does not make decisions about Data Subjects that produce legal or similarly significant effects. Segments, scores and attribution results produced by the Eyk Service are outputs for Customer's own use.

13. AI functions and external agents

13.1 The Eyk Service includes AI functions, such as the Eyk analytics agent, that use external model providers listed in the Subprocessor list. Customer enables AI functions in the platform and determines, through its access configuration, which users may use them and which data they may reach.

13.2 Access control defined in the Eyk semantic layer, per cube, dimension and metric, applies equally to in-product analytics, the analytics agent, the external API and MCP connections. AI functions are designed to retrieve only data the requesting user is permitted to access.

13.3 Eyk does not use Customer Data to train, fine-tune or improve its own or third-party models, and contracts with its model providers on terms under which Customer Data is not used for provider model training. Eyk may use aggregated and anonymised data, including to train and improve its own models, in accordance with Clause 14.

13.4 Prompts, responses, tool calls and agent actions are subject to access control, documented retention and logging appropriate to the sensitivity of the data. Eyk implements appropriate safeguards to protect Customer Data in AI functions and external agent connections.

13.5 AI functions do not take autonomous actions outside the Eyk Service, such as changing campaigns or budgets in third-party systems, unless Customer has enabled that action and it is logged.

13.6 Customer may connect external AI agents or tools (for example through the Eyk MCP server or API) using credentials issued to its users. Such a connection is Customer's instruction to transmit data to that tool; the tool's provider is Customer's own processor or recipient, not a Subprocessor of Eyk. Customer can disable an external connection at any time without affecting the rest of the Eyk Service.

13.7 The Subprocessor list names Eyk's model providers and their Processing locations. Changes follow Clause 9.

14. Aggregated and anonymised data

14.1 Customer instructs and authorises Eyk to create aggregated and anonymised data derived from Customer Data, which Eyk may use for benchmarking, product improvement, training and improving its own models, analytics about the use of the Eyk Service and industry insights, provided that neither Customer, its customers nor any natural person can reasonably be identified from that data, alone or in combination with other data.

14.2 Eyk documents its anonymisation method on request and does not attempt to re-identify anonymised data. Pseudonymised data is not anonymised data and remains Customer Data.

14.3 Eyk does not publish benchmarks that identify Customer or that allow Customer's figures to be inferred.

14.4 Aggregated and anonymised data is not Customer Data and may be retained after termination of the Agreement.

15. Audit and assurance

15.1 Eyk makes available the information necessary to demonstrate compliance with this DPA, including its trust center documentation, the Subprocessor list and, where available, independent assurance reports or certifications.

15.2 Audits start from that documentation. Where it is reasonably insufficient, or after a Personal Data Breach affecting Customer Data or a substantiated compliance concern, Customer may conduct an audit, itself or through an independent auditor that is bound by confidentiality and is not a competitor of Eyk, no more than once per 12 months unless required by a Supervisory Authority.

15.3 Where Eyk holds a current ISO/IEC 27001 certificate covering the Eyk Service, that certificate counts as sufficient documentation under Clause 15.2, unless there has been a Personal Data Breach affecting Customer Data or a substantiated compliance concern.

15.4 Audits are conducted with at least 30 days' notice, during business hours, limited to the systems and processes used for Customer Data, and without unreasonable disruption of Eyk's operations or access to other customers' data. Customer bears its own costs and Eyk's reasonable costs of audit support, unless the audit reveals a material breach of this DPA by Eyk.

15.5 This Clause does not limit the powers of a Supervisory Authority.

16. Data ownership, return and deletion

16.1 Customer retains ownership of and control over Customer Data. Nothing in this DPA transfers rights in Customer Data to Eyk, and nothing in it transfers Eyk's rights in the Eyk IP, as defined in the Terms and Conditions, to Customer.

16.2 During the term, Customer can export its data from the Customer Environment in documented, machine-readable formats through the data warehouse, the external API and the export functions of the Eyk Service.

16.3 On termination of the Agreement, Eyk keeps the Customer Environment available for export for 30 days, unless Customer requests earlier closure. Eyk ceases data flows to Destinations and revokes or returns API keys, OAuth grants and other credentials to Customer systems.

16.4 After that period, Eyk deletes Customer Data from production systems within 30 days and from backups through controlled rotation within 90 days, unless Union or Member State law requires retention, in which case the data is isolated and used for no other purpose. On request, Eyk confirms deletion in writing.

17. Liability

17.1 Eyk's liability under this DPA is subject to Clause 13 of the Terms and Conditions. Liability under this DPA counts towards the limit in that Clause and does not add to it.

17.2 Administrative fines imposed on Customer by a Supervisory Authority are excluded, except to the extent directly caused by Eyk's breach of this DPA and within that limit.

17.3 Each Party's liability towards Data Subjects under Article 82 GDPR is determined by that Article.

18. Term, changes and governing law

18.1 This DPA takes effect on acceptance of the Agreement and remains in force for as long as Eyk Processes Personal Data on behalf of Customer.

18.2 Eyk may update this DPA to reflect changes in law, regulatory guidance or the Eyk Service. Eyk gives at least 30 days' notice of material changes. If a change materially reduces Customer's protection, Customer may terminate the Agreement before the change takes effect. Termination on these terms is Customer's sole remedy.

18.3 Schedules 1 and 2 form part of this DPA. Eyk may update Schedule 2 in accordance with Clause 8.2 and the Subprocessor list in accordance with Clause 9.2.

18.4 If a provision of this DPA is invalid, the remaining provisions remain in force and the Parties replace the invalid provision with a valid one that most closely reflects its purpose.

18.5 This DPA is governed by Dutch law. Disputes are submitted to the court competent under the Terms and Conditions.

Schedule 1. Processing details

Item	Description
Subject matter	Provision and operation of the Eyk Service: first-party tracking and consent management, connectors, a data warehouse, dimensional data model, attribution and segmentation models, reporting, the analytics agent, the external API and MCP server, and customer support.
Purposes	Data integration, server-side tracking, conversion APIs, data quality monitoring, attribution, segmentation (including RFM), profitability and margin analysis, reporting and visualisation, marketing activation, support and onboarding of Customer's users. Training models on Customer Data is excluded (Clause 13.3); Eyk may train its own models on aggregated and anonymised data (Clause 14).
Nature	Collecting, transmitting, validating, combining, modelling, pseudonymising, attributing, segmenting, analysing, visualising, storing, activating, exporting, correcting, returning and deleting.
Duration	Term of the Agreement plus the return and deletion period in Clause 16.
Frequency	Batch, daily, near-real-time or on demand, depending on the source and function.
Data Subjects	Customer's consumers and customers; prospects, subscribers and website visitors; delivery recipients and return applicants; customer-care contacts; Customer's business contacts; Customer's Users, for activity records Eyk keeps for Customer, such as audit trails.
Hosting location	Customer Environment and its backups in the EEA; Subprocessors as stated in the Subprocessor list (Clauses 7.3 and 10).

Category	Examples	Note
Identification	Name, customer ID, user ID, order ID	Personal Data
Contact	Address, email, telephone	Personal Data
Commerce	Orders, products, discounts, returns	Personal Data when linked to a person
Marketing	Consent status, campaigns, opens, clicks	Personal Data; may involve profiling
Analytics / tracking	Events, client and user IDs, IP address, device, cookie and advertising identifiers, UTM	Personal Data where identifiable
Logistics	Shipment and fulfilment status	Personal Data
Financial indicators	Payment status, refunds, chargebacks, margin values	Personal Data; no full card data (PAN, CVC)
Derived	Segments, customer lifetime value, churn scores, attribution	Personal Data; profiling for Customer's use
Audit trails	User IDs and administrative events in the Customer Environment	Personal Data

Special categories of Personal Data, Personal Data relating to criminal convictions and offences, and HR data about Customer's employees or applicants are outside the scope of the Eyk Service unless agreed in writing. Eyk processes the account details, login and authentication data, usage and security logs and support messages of Customer's staff, and the data of billing contacts, as a controller under its privacy policy, not under this DPA.

Schedule 2. Technical and organisational measures

The measures below add to those in Clauses 6 to 9, 11, 13 and 16 and describe the outcomes Eyk maintains. Eyk decides how they are implemented and may replace individual measures by equivalent or stronger ones (Clause 8.2).

Domain	Measure
Encryption	Industry-standard encryption in transit and platform-supported encryption at rest, with controlled key access.
Secrets	Secrets managed through appropriate tooling; not exposed in source code or documentation.
Endpoints	Administrator endpoints protected against unauthorised access.
Secure development	Development, test and production separated; change control; dependency and secrets scanning; controlled deployment.
Logging and monitoring	Authentication, privileged access, administrative changes, exports, API activity and relevant agent actions logged where supported by the architecture; logs protected and retained proportionately.
Backup and recovery	Documented backup and recovery; periodic recovery testing.
Access control	Personal accounts with enforced two-step verification; access limited to what each role needs.
Joiners and leavers	Access granted and removed through a documented procedure and reviewed regularly.
Vulnerability management	Security alerts for the software Eyk uses monitored; critical and high risks fixed first.
Security testing	Regular security audits of Eyk’s code.
Incident response	Documented procedure for detecting, containing and reporting incidents (Clause 11).
Personnel	Confidentiality, training and need-to-know access (Clause 6).
Subprocessor management	Data-protection terms and notice of changes (Clause 9).
Business continuity	Continuity plan for critical systems and suppliers.