

DATA PROCESSING AGREEMENT

OBVELO — Personal Data Masking Gateway

Self-service version — accepted electronically at account registration

Version: 1.0 · **Published:** 2026-09-27 · **In force from:** 2026-09-27

This Data Processing Agreement (the "**DPA**") is concluded between:

Luminote P.S.A. (*prosta spółka akcyjna*), a company incorporated under the laws of the Republic of Poland, with its registered office at ul. Olszańska 7, 31-513 Kraków, Poland, entered in the Register of Entrepreneurs of the National Court Register (KRS) kept by the District Court for Kraków-Śródmieście in Kraków under number 0001223956, NIP 6751824986, REGON 543999032 (hereinafter referred to as the "**Processor**");

and

the business entity that registers an account for the Service and accepts this DPA, identified by the company name, registered address, country and VAT identification number (or other registration number) stored in its account (hereinafter referred to as the "**Customer**" or the "**Controller**"),

each a "**Party**" and together the "**Parties**".

Recitals

(A) The Processor provides OBVELO, a software service that sits between the Customer's applications and a language model provider (or other downstream system) chosen by the Customer, detects and masks personal data in the content sent through it, forwards the masked content, and restores the original values in the response.

(B) In providing OBVELO, the Processor processes personal data on behalf of the Customer. The Parties conclude this DPA to meet the requirements of Article 28 of Regulation (EU) 2016/679 (the "**GDPR**").

(C) The Service is designed to minimise the personal data it holds: the part of the Service that processes content stores nothing from that content, and the part that

manages accounts never receives it.

(D) The Service is offered on a self-service basis. This DPA is a standard agreement which forms an integral part of the Terms of Service and is concluded electronically when the Customer registers an account.

1. Conclusion of this DPA

1.1 Electronic conclusion. This DPA is concluded when the Customer, during registration of an account for the Service, confirms its acceptance of this DPA by ticking the relevant checkbox and completes the registration by confirming its e-mail address. The Parties agree that this constitutes the conclusion of a contract in writing, in electronic form, within the meaning of Article 28(9) GDPR, which is an autonomous concept of Union law. No handwritten or qualified electronic signature is required. For the purposes of Polish law, this DPA is concluded in documentary form (*forma dokumentowa*, Article 77² of the Polish Civil Code).

1.2 Availability before conclusion. The Processor makes this DPA available before registration, via a link in the registration form and at <https://app.obvelo.com/legal/dpa>, in a manner which allows the Customer to download, store and reproduce it (PDF and HTML). Immediately after the e-mail address is confirmed, the Processor sends the accepted version of this DPA to the Customer's Account e-mail address as a PDF attachment, which constitutes a durable medium, and keeps it permanently available in the customer panel.

1.3 Record of acceptance. The Processor keeps a record of each acceptance, including the account identifier, the accepted DPA version, the date and time of acceptance and the e-mail address used. This record serves as evidence of the conclusion of this DPA and its content.

1.4 Business customers only. The Service and this DPA are intended exclusively for entrepreneurs and other entities acting in the course of business. By accepting this DPA, the person registering the account represents that they are authorised to conclude it on behalf of the Customer.

1.5 All plans. This DPA applies to every plan offered by the Processor on a self-service basis (Free, Starter, Standard and Pro). A Customer on the Enterprise plan, or with a Customer-hosted deployment, may conclude an individually negotiated data processing agreement, which, once signed, replaces this DPA for that Customer.

1.6 No separate signature. No handwritten or qualified electronic signature is required for this DPA to be valid. On request, the Processor will provide the Customer with a countersigned copy of the version accepted by the Customer.

2. Definitions

2.1 Terms such as "personal data", "processing", "controller", "processor", "data subject", "personal data breach", "supervisory authority" and "special categories of personal data" have the meanings given in the GDPR.

2.2 In this DPA:

"Terms of Service" means the terms of service of OBVELO published by the Processor at <https://app.obvelo.com/legal/terms>, together with the plan selected by the Customer in its account.

"Service" or **"OBVELO"** means the OBVELO service provided by the Processor, in any of its deployment shapes and surfaces, including: (a) the gateway used by replacing the base URL of a language model provider (**"Proxy Mode"**); (b) the masking API (`/v1/mask` , `/v1/restore` , `/v1/inspect`) together with the client-side SDK (**"API Mode"**); (c) the MCP tool gateway; (d) the web page for pasting text or uploading documents (`/app`); (e) the browser extension; and (f) the customer panel.

"Account" means the Customer's account in the Service, created at registration.

"Data Plane" means the part of the Service that receives and processes the content of Requests: the gateway, the Name Recognition Model and, for plans that include it, the component that reads scanned documents and images (**"OCR Component"**).

"Control Plane" means the part of the Service that manages Accounts, API keys, plans, usage metering, billing and Tenant Configuration. The Control Plane does not receive the content of Requests.

"Request" means any content sent by or on behalf of the Customer to the Data Plane, including text, JSON payloads, tool-call arguments, API responses and file attachments, together with any per-request options (including per-request dictionaries, lists of values to mask or not to mask, and patterns).

"Response" means the content returned through the Data Plane to the Customer, including responses from a Third-Party Model Provider passing back through the gateway.

"Customer Personal Data" means personal data contained in Requests, Responses and Tenant Configuration, and the browser extension activity described in Section 5.8, that the Processor processes on behalf of the Customer in providing the Service.

"Token Map" means the correspondence between placeholder tokens (e.g. `[Person 1]`) and the original values replaced by them.

"Tenant Configuration" means settings saved by the Customer for its Account in the customer panel, including: jurisdiction scoping (countries); enabling, disabling and grouping of detection rules, categories and labels; custom patterns; the attachment policy; the coverage profile; the name-recognition setting; coreference and inflection settings; the maximum request size within the plan; whether forwarding to a language model is permitted; the address of the Customer's own model endpoint (where the plan allows it); agent profiles and tool policies; and the assignment of an agent profile to an API key. Lists of values to mask or not to mask and dictionaries of names are **not** stored: they travel with each Request.

"Name Recognition Model" means the person-name recognition model used by the Service (**SITO**), developed and owned by the Processor, which holds all rights to the model and its weights, including the right to license them for Customer-hosted deployments. It runs within the Processor's own container image without network access. No other name-recognition model is used to provide the Service.

"Third-Party Model Provider" means any language model provider or other downstream endpoint to which the Customer directs the Service to forward masked Requests, using credentials of the Customer (e.g. OpenAI, Anthropic, Google, Mistral, Azure OpenAI or a self-hosted model).

"Sub-processor" means any third party engaged by the Processor that processes Customer Personal Data on behalf of the Processor.

"Data Protection Laws" means the GDPR, the Polish Act of 10 May 2018 on the Protection of Personal Data, and any other data protection law of the European Union or its Member States applicable to the processing under this DPA.

"EEA" means the European Economic Area.

3. Scope and roles of the Parties

3.1 Processor role. With respect to Customer Personal Data, the Customer acts as controller (or as processor on behalf of its own clients, in which case the Processor acts as its sub-processor) and the Processor acts as processor. Annex I describes the processing.

3.2 Account and billing data. The Processor processes the personal data of the Customer's contact persons and Account users that is needed to administer the Terms of Service (such as e-mail addresses, invoicing data, subscription and payment history, usage counters) as an independent controller, for the purposes of concluding and performing the Terms of Service, billing, accounting, tax compliance and service

security. That processing is governed by the Processor's Privacy Policy at <https://app.obvelo.com/legal/privacy> and falls outside this DPA.

3.3 Third-Party Model Providers. The Customer selects the Third-Party Model Provider, contracts with it directly, and supplies its own credentials, which pass through the Service without being substituted. The Processor does not call any language model under its own contract. Accordingly:

(a) a Third-Party Model Provider is **not** a Sub-processor of the Processor; it is a recipient chosen by the Customer, and its processing is governed by the Customer's own agreement with it;

(b) by sending Requests to the gateway's path for a Third-Party Model Provider, or by configuring its own model endpoint in its Tenant Configuration, the Customer expressly instructs the Processor to forward masked Requests to that endpoint; such forwarding constitutes processing on the Customer's documented instructions, and the disclosure to the Third-Party Model Provider is a disclosure by the Customer as controller;

(c) the Customer bears sole responsibility for its legal relationship with each Third-Party Model Provider, including the lawful basis for the disclosure, the data processing agreement, and any transfer mechanism required under Chapter V GDPR (such as an adequacy decision or standard contractual clauses);

(d) the Processor is not responsible for the processing carried out by any Third-Party Model Provider, including its retention, use for model training, security or transfers of data.

3.4 Customer-hosted deployment. Where the Service is deployed within the Customer's own infrastructure (its private cloud or its own premises), the Processor does not have access to Customer Personal Data in the ordinary course, and this DPA applies only to the extent the Processor accesses Customer Personal Data, e.g. when providing support at the Customer's request.

3.5 Use without a language model. Where the Customer uses the Service without any Third-Party Model Provider (API Mode or file masking only), no Customer Personal Data is forwarded to any external model endpoint by the Service.

4. Instructions

4.1 The Processor processes Customer Personal Data only on documented instructions from the Customer, including with regard to transfers to third countries, unless required to do so by Union or Member State law to which the Processor is

subject; in such a case the Processor informs the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.2 The Customer's documented instructions consist of: (a) this DPA and the Terms of Service; (b) the Customer's configuration and use of the Service, including Tenant Configuration, per-request options, the choice of Third-Party Model Provider and the attachment policy; and (c) any further instructions sent by the Customer from its Account e-mail address to security@obvelo.com and accepted by the Processor in writing or electronic form.

4.3 The Processor shall immediately inform the Customer if, in its opinion, an instruction infringes Data Protection Laws. The Processor may suspend the performance of such an instruction until it is confirmed or amended by the Customer.

4.4 The Processor shall not process Customer Personal Data for its own purposes, including for training or improving the Name Recognition Model or any other model, for building dictionaries, or for creating datasets.

5. Data-minimising design of the Service

5.1 **No retention of Request content.** The Data Plane stores nothing from the content of Requests or Responses: not the content, not Token Maps, not per-request dictionaries, lists or patterns. Such content is held only in memory for the time necessary to process the Request and return the Response. Core dumps are disabled for every Data Plane process that handles Request content, so that content is never written to disk by a process failure.

5.2 **Token Maps.** In Proxy Mode the Token Map needed to restore values exists only in memory for the duration of the Request and is discarded after the Response is returned. In API Mode and in the MCP tool gateway the Token Map is returned to the Customer, which keeps it on its own side and sends it back with the next Request where needed; restoration is performed by the Customer's application or the SDK. The Processor keeps no copy.

5.3 **Logs.** Operational and compliance logs of the Data Plane do not contain the content of Requests or the original values replaced by tokens. They may contain metadata such as timestamps, the Account and API key identifiers, the agent profile and the names of tools declared in a Request, detection categories and counts, character counts, attachment descriptors (type, media type, size, position in payload — never file contents), and the browser extension events described in Section 5.8. The Data Plane does not record source IP addresses. Data Plane logs are kept only in

rotating files limited by size — at most 50 MB per container of the Data Plane (five files of 10 MB) — in which the oldest entries are overwritten by new ones; they are not archived, forwarded or copied elsewhere, and are deleted with the container.

5.4 Counters. Rate and usage counters are numbers stored under the Account identifier and a time window. They contain no personal data from Requests. Usage counters needed for billing (characters and pages per Account and period) are kept in the Control Plane.

5.5 Separation of planes. The Control Plane never receives the content of Requests. The container image of the Data Plane does not include Control Plane code or its sub-processors. This separation is enforced by automated tests.

5.6 Name Recognition Model and OCR Component. The Name Recognition Model and the OCR Component run within the Processor's container images and have no network access. No third party is involved in person-name recognition or in reading scanned documents.

5.7 Browser-side dictionaries. Dictionaries and lists created in the browser extension are stored locally in the user's browser and are transmitted to the Service only as part of a masking Request.

5.8 Browser extension activity. Where the Customer uses the administrator mode of the browser extension, the Data Plane receives events from a closed list — the extension being active, paused or resumed, a chat site added or removed (host name only), a file sent without masking (file type only, never its name or content), an administrator sign-in, the names of changed settings, the number of dictionary entries loaded, and uninstallation — together with a random installation identifier. The events contain no content and no names. Each gateway instance keeps them in memory for up to 30 days (at most 10,000 events per Account) and prints them as log lines subject to Section 5.3; the customer panel reads them on request and stores nothing.

5.9 Tenant Configuration. Tenant Configuration is stored in the Control Plane for as long as the Account exists. To the extent the Customer includes personal data in it (e.g. a custom pattern naming a person), that data is Customer Personal Data and is processed under this DPA.

6. Nature of the masking functionality; Customer responsibilities

6.1 Risk-reduction measure. The Service is a technical measure intended to reduce the amount of personal data disclosed to Third-Party Model Providers and other recipients. Detection is based on deterministic rules and a statistical model and is not exhaustive. The Processor does not warrant that every item of personal data in a Request will be detected and masked, nor that use of the Service alone ensures the Customer's compliance with Data Protection Laws. The Customer remains responsible for assessing whether the Service, as configured, is appropriate to its processing, including in any data protection impact assessment. With respect to detection, the Processor's obligation is to exercise due diligence in providing the Service in accordance with its documentation (an obligation of means), not to achieve a particular result.

6.2 Documented limitations. The Processor describes the known limitations of the Service in its documentation at <https://obvelo.com/docs/#limits> and keeps that description up to date. As at the date of this version, these include in particular:

- (a) a file referenced by identifier (e.g. `file_id`) never passes through the Service; the Third-Party Model Provider retrieves it directly, and the Service reports the reference;
- (b) file attachments are masked only under the `mask` attachment policy; under the default `flag` policy they are forwarded unmasked and the Response reports them;
- (c) under the `mask` policy, Office files (docx, xlsx, pptx and similar), csv and plain text are masked on every surface; a PDF with a text layer is returned as masked **text** (not as a PDF) and only through the `object` field of `/v1/mask`; a scanned document or an image is read only on plans with the OCR add-on and only through that field; on the model gateway a PDF or an image is forwarded unmasked and reported; an encrypted PDF is never masked; OCR reads at most 20 pages per file;
- (d) a Request sent in the `text` field of `/v1/mask` does not mask files, because the masked file has no way to be returned; the Response says so;
- (e) values read by OCR from a damaged or low-quality scan may be read incorrectly and then may not be recognised;
- (f) names of cities and towns are masked only when the Customer selects the extended coverage profile or the corresponding rule group;
- (g) the business name of a sole trader, which contains the owner's surname, is masked reliably only when the Customer supplies its list of counterparties with the Request;
- (h) tools that the language model calls directly, outside the Service, do not pass through the Service;

(i) detection accuracy may be lower for languages and document types outside the measured set.

6.3 Attachment policy. The Customer selects the policy applied when a Request contains an attachment: `block` (the Request is refused), `flag` (the attachment is forwarded unmasked and the Response reports it) or `mask`. The default is `flag`. Keeping or selecting `flag` constitutes the Customer's informed decision that attachments may be forwarded without masking.

6.4 After restoration. Once values are restored in a Response, the restored content is under the Customer's control. The Processor has no visibility of, and no responsibility for, any further use or transmission of that content by the Customer's applications or tools, including tools the language model calls directly outside the Service.

6.5 Customer obligations. The Customer shall: (a) ensure it has a lawful basis for the processing of Customer Personal Data and for its disclosure to any Third-Party Model Provider; (b) provide any information to data subjects required by Data Protection Laws; (c) keep its API keys and model provider credentials confidential and revoke compromised keys without delay; (d) configure the Service in a manner appropriate to the categories of data it processes, including enabling identifier rules relevant to its sector and the `mask` attachment policy where attachments contain personal data; (e) keep the Account e-mail address and company data up to date, as they are used for all notices under this DPA.

7. Confidentiality

7.1 The Processor shall ensure that persons authorised to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and that they process Customer Personal Data only as necessary to provide the Service.

7.2 Access to production systems of the Data Plane is limited to personnel who need it for operating, securing and supporting the Service.

8. Security of processing

8.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risks for the rights and freedoms of natural persons, the Processor shall implement and maintain

appropriate technical and organisational measures pursuant to Article 32 GDPR, including the measures described in **Annex II**.

8.2 The Processor may update the measures in Annex II, provided that the overall level of protection is not reduced.

9. Sub-processors

9.1 **General authorisation.** The Customer grants the Processor a general written authorisation to engage Sub-processors. The Sub-processors engaged as at the date of this version are listed in **Annex III**; the current list is published in Annex III of this DPA at <https://app.obvelo.com/legal/dpa>.

9.2 **EEA only.** The Processor shall engage only Sub-processors that process Customer Personal Data within the EEA.

9.3 **Changes.** The Processor shall inform the Customer of any intended addition or replacement of a Sub-processor at least **30 days** in advance, by e-mail to the Account e-mail address and by a notice in the customer panel. The Customer may object to the change on reasonable grounds relating to data protection within that period, by e-mail to security@obvelo.com. If the Parties do not resolve the objection, the Customer may terminate the Terms of Service with effect before the change takes place, and the Processor shall refund any prepaid fees for the period after termination.

9.4 **Sub-processor obligations.** The Processor shall impose on each Sub-processor, by way of a contract, data protection obligations substantially equivalent to those in this DPA, in particular providing sufficient guarantees to implement appropriate technical and organisational measures. The Processor remains fully liable to the Customer for the performance of each Sub-processor's obligations.

10. Transfers outside the EEA

10.1 The Processor shall not transfer Customer Personal Data outside the EEA and shall not permit its Sub-processors to do so. This is a deliberate feature of the Service. Any change to this rule may be made only by amendment of this DPA under Section 16.2, with the Customer's right to terminate before the change takes effect.

10.2 Forwarding of masked Requests to a Third-Party Model Provider located outside the EEA, where so directed by the Customer, is a disclosure made on the Customer's

instruction to a recipient chosen by the Customer (Section 3.3). The Customer is responsible for ensuring that any such transfer complies with Chapter V GDPR.

10.3 Section 10.1 does not apply to Account and billing data processed by the Processor as an independent controller (Section 3.2), which is governed by the Privacy Policy.

11. Assistance to the Customer

11.1 Data subject requests. Taking into account the nature of the processing, the Processor shall assist the Customer by appropriate technical and organisational measures, insofar as possible, in fulfilling its obligation to respond to requests for exercising data subject rights. Because the Data Plane does not retain the content of Requests, the Processor will generally not hold Customer Personal Data from Requests to which such a request could relate; the Processor shall confirm this in writing upon request. If the Processor receives a request directly from a data subject relating to Customer Personal Data, it shall forward it to the Customer without undue delay and shall not respond itself except to confirm that the request was forwarded.

11.2 Other assistance. The Processor shall assist the Customer in ensuring compliance with Articles 32 to 36 GDPR, taking into account the nature of processing and the information available to the Processor, including by providing information on the Service's architecture and measured detection performance for the Customer's data protection impact assessments and prior consultations.

11.3 Assistance going beyond providing existing documentation may be charged at the Processor's then-current rates, agreed in advance, unless it results from the Processor's breach of this DPA.

12. Personal data breaches

12.1 The Processor shall notify the Customer without undue delay, and in any event within **48 hours**, after becoming aware of a personal data breach affecting Customer Personal Data. Notifications are sent to the Account e-mail address and, where available, to a security contact designated by the Customer in the customer panel.

12.2 The notification shall, to the extent then known, describe: the nature of the breach, including the categories and approximate number of data subjects and records concerned; the likely consequences; the measures taken or proposed to address the breach and mitigate its possible adverse effects; and a contact point.

Where not all information is available at once, the Processor shall provide it in phases without undue further delay.

12.3 The Processor shall take reasonable steps to contain and remedy the breach and shall cooperate with the Customer in its notifications to the supervisory authority and to data subjects. Notification of a breach is not an acknowledgement of fault or liability.

12.4 For the avoidance of doubt, the non-detection of an item of personal data by the masking functionality, when the Service operated as documented, is not in itself a personal data breach on the part of the Processor.

13. Audits and information

13.1 The Processor shall make available to the Customer all information necessary to demonstrate compliance with Article 28 GDPR and this DPA, including a description of the architecture, the list of Sub-processors, a summary of security measures and, where available, test and measurement reports concerning the Service. Standard documentation is available at <https://obvelo.com/docs/#data> or on request to security@obvelo.com.

13.2 Audits shall be carried out primarily by means of the documentation referred to in Section 13.1 and by written questionnaires, which the Processor shall answer within 30 days. A remote audit (review of additional documents, interviews, demonstration of controls by video call) may be requested where the documentation and answers are demonstrably insufficient. An on-site audit at the Processor's premises is permitted only where (i) the documentation, answers and remote audit are demonstrably insufficient to demonstrate compliance with Article 28 GDPR, (ii) it is required by a competent supervisory authority, or (iii) it follows a personal data breach affecting Customer Personal Data. Data centres of Sub-processors are not subject to on-site audits by the Customer (Section 13.3). Any audit may be conducted by the Customer or an independent auditor mandated by the Customer and bound by confidentiality, who is not a competitor of the Processor, and is subject to the following: (a) at least **30 days'** written notice, except where required by a supervisory authority or following a personal data breach; (b) no more than once in any 12-month period, save for the above exceptions; (c) during business hours and without unreasonably disrupting the Processor's operations; the auditor shall have no access to data of other customers, to source code, or to information whose disclosure would compromise the security of the Service, and information obtained in an audit is confidential information of the Processor; (d) each Party bears its own costs, unless the audit reveals a material breach of this DPA by the Processor.

13.3 Audits of Sub-processors shall be carried out primarily by means of documentation, certificates and reports available from those Sub-processors.

14. Deletion and return

14.1 Content of Requests is deleted in the ordinary course upon completion of each Request, as described in Section 5.

14.2 Upon closure of the Account or termination of the Terms of Service, the Processor shall delete Tenant Configuration and any other Customer Personal Data held by the Processor within **30 days**, unless Union or Member State law requires storage. Before closing the Account, the Customer may copy its Tenant Configuration from the customer panel, where it is shown in full as a structured (JSON) document, or request a copy by e-mail. Copies in backups shall be deleted in accordance with the regular backup rotation cycle, which does not exceed **30 days**, and shall not be restored for any purpose in the meantime. As a result, all Customer Personal Data is erased within 60 days of Account closure.

14.3 The Processor shall confirm the deletion in writing upon request.

15. Liability

15.1 Each Party's liability arising out of or in connection with this DPA is subject to the limitations and exclusions of liability set out in Section 14 of the Terms of Service, to the extent permitted by Data Protection Laws. Liability under this DPA and under the Terms of Service is aggregated and subject to one common limit. Nothing in this DPA limits either Party's liability towards data subjects under Article 82 GDPR.

16. Term, changes and termination

16.1 This DPA enters into force upon its conclusion under Section 1 and remains in force for as long as the Processor processes Customer Personal Data under the Terms of Service, including the deletion period under Section 14.

16.2 **Changes to this DPA.** The Processor may amend this DPA for important reasons, such as changes in Data Protection Laws, guidance of supervisory authorities, or changes to the Service. The Processor shall notify the Customer of the

amended version by e-mail to the Account e-mail address and in the customer panel at least **30 days** before it takes effect, stating the changes. If the Customer does not accept the amended version, it may terminate the Terms of Service with effect before the amended version takes effect. Continued use of the Service after that date constitutes acceptance of the amended version. Amendments required by law may take effect earlier where the law so requires. Updates of Annex II and Annex III made in accordance with Sections 8.2 and 9.3 do not constitute amendments under this Section.

16.3 Version history. All previous versions of this DPA remain available on the Processor's website, each under its own address (for example <https://app.obvelo.com/legal/dpa-1.0.html>), with their dates of validity.

16.4 Obligations which by their nature should survive termination (in particular Sections 7, 12, 14 and 15) survive the termination of this DPA.

17. Governing law and jurisdiction

17.1 This DPA, and any non-contractual obligations arising out of or in connection with it, is governed by the laws of the Republic of Poland.

17.2 Any disputes arising out of or in connection with this DPA shall be resolved exclusively by the common court having jurisdiction over the registered office of the Processor, i.e. the competent common court in Kraków, Poland.

17.3 This Section does not affect the right of any data subject or Party to lodge a complaint with a competent supervisory authority, including the President of the Personal Data Protection Office (*Prezes Urzędu Ochrony Danych Osobowych*), or the jurisdiction of courts under Article 79 GDPR.

18. Final provisions

18.1 Order of precedence. In the event of any conflict between this DPA and the Terms of Service concerning the processing of Customer Personal Data, this DPA prevails.

18.2 Notices. Notices to the Customer are sent to the Account e-mail address and published in the customer panel. Notices to the Processor are sent to security@obvelo.com. A notice sent by e-mail is deemed received on the next business day after sending.

18.3 **Severability.** If any provision of this DPA is found invalid, the remaining provisions remain in force, and the Parties shall replace the invalid provision with a valid one that most closely achieves its purpose.

18.4 **Language.** This DPA is concluded in English. If a translation is made available, the English version prevails.

ANNEX I — Description of the processing

Item	Description
Subject matter	Provision of OBVELO: detection and masking of personal data in content sent by the Customer, forwarding of masked content to an endpoint chosen by the Customer, and restoration of original values in the response; storage of Tenant Configuration; for the browser extension's administrator mode, the activity events in Section 5.8.
Duration	For as long as the Account exists. Content of Requests: only for the duration of processing of each Request. Browser extension activity: up to 30 days. Tenant Configuration: until deletion under Section 14.
Nature of processing	Receipt, analysis (rule-based pattern matching and person-name recognition with a locally run model), replacement with tokens, transmission to the Customer-directed endpoint, restoration, return to the Customer; when the <code>mask</code> policy is selected: unpacking of Office files and masking of text, attributes and metadata, and reassembly; extraction of the text layer of PDF files and, on plans with the OCR add-on, optical character recognition of scans and images, returned as masked text; storage of Tenant Configuration.
Purpose	Reducing the disclosure of personal data by the Customer to Third-Party Model Providers and other systems, and inspecting content for personal data at the Customer's request.

Item	Description
Categories of data subjects	Determined by the Customer. Typically: the Customer's employees and collaborators; the Customer's clients, patients, citizens, prospects and their representatives; counterparties and suppliers; any other natural persons whose data appear in content the Customer sends through the Service. For Section 5.8: the Customer's users of the browser extension.
Categories of personal data	Determined by the Customer. May include: names and surnames; contact data (e-mail addresses, telephone numbers, postal addresses); national identification numbers (e.g. PESEL and equivalents), tax and VAT numbers, passport, identity card, driving licence and residence document numbers; health insurance, patient and clinician numbers; bank account numbers (IBAN and national formats), payment card numbers; vehicle registration numbers; online identifiers; file metadata (author, editor, reviewer names); any other personal data contained in free text, documents, scans, tool-call arguments or API responses. For Section 5.8: a random installation identifier and administrator sign-in events.
Special categories	The Customer may send content containing special categories of personal data (e.g. health data, medical record numbers) or data relating to criminal convictions. Such data is processed only transiently as part of the Request. The Customer shall assess the appropriateness of the Service for such data and configure it accordingly.
Frequency	Continuous, on each Request made by the Customer.
Place of processing	EEA only (see Annex III). In Customer-hosted deployments: the Customer's infrastructure.

ANNEX II — Technical and organisational measures

A. Data minimisation and architecture

1. The Data Plane stores nothing from Request content, Response content, Token Maps or per-request dictionaries and lists; content is processed in memory only.
2. Logical and code-level separation between the Data Plane and the Control Plane; the Data Plane image does not include Control Plane code or its sub-

processors; enforced by automated tests.

3. Logs do not contain the content of Requests or original values; attachment descriptors never include file contents; the Data Plane does not record source IP addresses.
4. The Name Recognition Model (SITO) and the OCR Component run in containers with no network (`network_mode: "none"`), enforced by automated tests. No other name-recognition model is part of the Service; this is enforced by automated tests of the deployment files and by the model container refusing to start any other engine.
5. Customer credentials for Third-Party Model Providers pass through the gateway without being substituted; the gateway only connects to model hosts on an allow-list set in the network permissions of the image, so it cannot act as an open relay.
6. The Customer can disable forwarding to any language model for its Account and for each agent profile; a Request can select only among the Customer's own agent profiles, so it cannot enable forwarding that the Customer's own settings do not allow. An agent profile can be pinned to an API key.
7. Structural keys (identifiers, cursors, pagination) are preserved to keep integrations working, while identifiers next to identity labels (e.g. patient ID, national ID) are always masked.

B. Access control and key management

1. Access to the Service by API keys; keys can be issued and revoked by the Customer; revocation takes effect at the next configuration refresh of the Data Plane (every 60 seconds). If the Control Plane is unreachable, the Data Plane continues with its last configuration, and revocation takes effect once it is reachable again.
2. Per-Account limits on request rate and body size, shared by all the Account's keys; hard usage limits enabled by default.
3. Account status enforcement: suspended Accounts, including those suspended for a failed payment, are blocked from the Data Plane.
4. Account registration requires confirmation of the e-mail address before an API key can be issued.
5. Administrative access to production servers restricted to authorised personnel, using SSH public-key authentication.

C. Transmission and web security

1. Encryption in transit using TLS for all public endpoints.
2. Customer-facing web pages use a Content Security Policy restricting connections to the same origin (`connect-src 'self'`); no third-party scripts, fonts or analytics are loaded. The sign-in pages are served by the identity

service with its own security headers and load no third-party scripts, fonts or analytics.

3. Own mail server with DKIM for Account e-mails.

D. Integrity, availability and resilience

1. Control Plane database backed up hourly, checked for integrity, encrypted (AES-256 with a PBKDF2-derived key) and kept for 30 days; the backup-and-restore path is exercised by an automated test.
2. Service components run under a supervised process manager with automatic restart and health checks; operational logs are reviewed by the operator.

E. Testing and quality

1. Detection rules are deterministic and versioned; changes to rules and models are accepted only after measurement against fixed test corpora, including corpora annotated by third parties, with a minimum specificity threshold.
2. Automated regression tests covering leakage (unmasked values reaching the output), destruction of non-personal values and fidelity of restoration; guards verified by deliberately breaking the code they protect.
3. Detected limitations are documented and disclosed to customers (see Section 6.2).

F. Organisational measures

1. Confidentiality obligations for all personnel with access to Customer Personal Data.
2. Record of processing activities maintained under Article 30(2) GDPR.
3. Sub-processor register maintained; new sub-processors added to the register before deployment.
4. The Processor maintains a written incident response procedure consistent with Section 12, handles vulnerability reports received at security@obvelo.com under a written procedure, and tests every change to the Service automatically before it is deployed.

ANNEX III — Sub-processors

Sub-processor	Service	Location of processing	Data concerned
OVH Sp. z o.o. , ul. Powstańców Śląskich 9, 53-	Hosting of Data Plane and Control	Current: Data Plane — OVHcloud, Roubaix, France; Control Plane —	Request content (transient, in memory); browser

Sub-processor	Service	Location of processing	Data concerned
332 Wrocław, Poland, KRS 0000220286, NIP 8992520556 (member of the OVHcloud group)	Plane infrastructure	OVHcloud, Warsaw, Poland. Additional locations authorised in advance: OVHcloud data centres in France, Poland and Germany.	extension activity (Section 5.8); Tenant Configuration; backups of the Control Plane

Additional locations. The Customer authorises the Processor to process Customer Personal Data, through the Sub-processor listed above, in any of the locations listed above. The Processor shall inform the Customer in the customer panel and in Annex III of this DPA at <https://app.obvelo.com/legal/dpa> before Customer Personal Data are first processed in an additional location. Adding any location not listed above, or any location outside the EEA, is not permitted under this authorisation and is subject to Sections 9.2 and 9.3.

Not Sub-processors (for clarity):

- **Name recognition and OCR:** performed by the Processor's own components on the Processor's infrastructure, without network access; no third party is involved.
- **Third-Party Model Providers:** chosen and contracted by the Customer, accessed with the Customer's credentials (Section 3.3).
- **E-mail:** Account e-mails are sent from the Processor's own mail server; no third-party e-mail delivery service is involved.
- **Identity service:** sign-in to the customer panel runs on identity software operated by the Processor on its own infrastructure; no third party is involved.
- **Payment provider — Mollie B.V.,** Keizersgracht 126, 1015 CW Amsterdam, the Netherlands: processes only Account and billing data for which the Processor is an independent controller (Section 3.2); it never receives the content of Requests.