Data processing agreement

Version 2026-10-08 · following the structure of the Danish Data Protection Agency's standard contractual clauses

1. The parties

The data controller: [VIRKSOMHEDENS NAVN], CVR [VIRKSOMHEDENS CVR], [VIRKSOMHEDENS ADRESSE] (hereinafter "the controller" or "the company").

The data processor: AI Optimize ApS, CVR 44389908, Midtager 33, 2605 Brøndby, support@autora.nu (hereinafter "the processor" or "Autora").

The parties have entered into this data processing agreement (hereinafter "the agreement") to meet the requirements of Article 28(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the General Data Protection Regulation, "GDPR").

2. Background and purpose

The processor provides a CRM platform as an online service (software as a service) in which the company records and processes information about its customers, contact persons, leads, tasks, appointments, documents, quotes, signatures, time tracking, emails and, when the module is turned on, information for customer due diligence under the Danish anti-money laundering act (KYC).

The company is the controller of the personal data it records in the platform and lets its customers submit through the customer portal. The processor processes the data on behalf of the company and on its instructions.

The processor is an independent controller of information about the company's own users (staff accounts: name, email, password in hashed form, two-factor setup, login times and IP addresses used to limit attempts) to the extent the processing is carried out to operate, secure and invoice the service. That processing is described in the processor's privacy policy.

3. Instructions

The processor may only process personal data on documented instructions from the controller, unless required to do so by EU or national law to which the processor is subject. In that case the processor informs the controller of the legal requirement before processing, unless the law prohibits this on important grounds of public interest.

The instructions are the company's use of the platform's features: creating, editing, viewing, exporting, anonymising and deleting records, sending emails and documents, automation that the company itself has turned on and configured, the customer portal, customer due diligence (including automatic screening against public sanctions and PEP lists when the company has turned it on) and the integrations (payments, bookkeeping, company register lookups) that the company itself connects. The processor does not process the data for its own purposes.

The processor immediately informs the controller if, in the processor's opinion, an instruction infringes the GDPR or other data protection law.

4. Categories of data subjects and personal data (annex A)

The processing covers the following categories of data subjects and data, depending on the modules the company has turned on:

- The company's customers and their contact persons: name, address, email, phone, company registration (CVR) number, customer number, role, status, custom fields, notes, timeline and correspondence (sent emails).
- Leads from the web form, booking and import: name, company, email, phone, message and status.
- Users of the customer portal: email, password (hash only), login times, messages, uploads and answers.
- Customer due diligence (KYC, anti-money laundering act), when the module is turned on: questionnaire answers (including whether a person is politically exposed), beneficial owners (name and role), identity documents (e.g. passport, driving licence, health insurance card), company register extracts, results of screening against public sanctions and PEP lists (possible matches, staff assessments and screening reports), risk assessment, approvals and internal notes. Data about criminal convictions is not processed; information about political exposure is sensitive in its context and is restricted to roles with access to KYC.
- Quotes and signatures: the recipient's name and email, the document's content, the time of signing, IP address and browser details as evidence.
- Payments and bookkeeping, when the modules are turned on: the customer's name and email at Stripe, amounts, status and dates; entries and missing vouchers from e-conomic.
- Time tracking: the employee's entries per customer and task.

- The company's own staff as users: name, email, role, title, phone, two-factor status and actions in the audit log.

5. Obligations of the processor

The processor processes the data only for the purposes and by the means set out in the instructions, and only for as long as the agreement is in force.

The processor ensures that access to personal data is limited to the persons who need it to deliver and operate the service (platform administrators), and that these persons are bound by confidentiality.

The processor maintains a record of the categories of processing carried out on behalf of the controller, cf. GDPR Article 30(2).

6. Confidentiality

The processor ensures that persons authorised to process personal data on behalf of the controller have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. The confidentiality continues after the end of employment or cooperation.

The processor grants access to personal data only to persons with a work-related need and can, on request, document who has access to the production environment.

7. Security of processing (annex C)

The processor implements appropriate technical and organisational measures under GDPR Article 32, taking into account the state of the art, the costs and the nature, scope, context and purposes of the processing as well as the risks for the data subjects. The measures include at least:

- Hosting in the EU with separation between companies in the application layer: every query is filtered on the company's id, and the separation is tested automatically in test runs.
- Encryption in transit (TLS) and encryption of uploaded files and stored secrets at rest (AES-256-GCM).
- Passwords are stored only as hashes; two-factor login (TOTP) can be turned on and can be required for roles with access to KYC; login and login-link attempts are rate limited.
-

Roles and permissions per company; KYC information is visible only to roles with access to KYC, also in the audit log, notifications, files and exports.

- An audit log of changes to data and settings (Settings ’ Log) and export of it.
- Database and files on persistent storage in the EU with ongoing backups, so the data can be restored after a failure, and testing of the restore.
- Monitoring of the service (/api/health), error reporting without customer data, and personal one-time links in emails that are masked in the outbox.
- Deletion and anonymisation per customer, export of all the company's data and deletion of the whole company as product features.

8. Sub-processors (annex B)

The controller gives a general authorisation for the processor to use sub-processors. The processor enters into a written agreement with each sub-processor imposing the same data protection obligations as this agreement, and remains fully liable to the controller for the sub-processor's performance of them.

The processor informs the controller of intended additions or replacements of sub-processors at least 30 days before the change takes effect (through an updated version of this agreement in the system and a notification to the company's owner). The controller may object before the change; if the parties cannot agree, the controller may terminate the agreement and export and delete its data, cf. section 12.

The following sub-processors and recipients are used at the time of signing:

- Railway Corporation (sub-processor): Hosting of the application, the database (Postgres) and uploaded files. Location: Data centre in the EU (Railway's region europe-west4, Amsterdam, the Netherlands). Transfer: Data is stored in the EU. The company is US-based; any access from the US (e.g. support) relies on the European Commission's standard contractual clauses (Decision 2021/914) in Railway's data processing addendum.
- Simply.com A/S (CVR 29412006) (sub-processor): Sending emails through the platform's mail account (SMTP): recipient address, name, subject and content. Location: Denmark (EU). Transfer: No transfer to third countries. Only emails sent through the platform. If the company sends through its own mail account (SMTP), emails go directly from the company's own mail provider, which is not a sub-processor of the platform.

- Stripe Payments Europe, Ltd. / Stripe, Inc. (sub-processor): Payments and subscriptions (the Payments module): the customer's name, email and payment details are processed by Stripe; the platform keeps copies of status, amounts and dates. Location: Ireland (EU); Stripe, Inc. in the USA. Transfer: Stripe's own transfer mechanisms (the EU-U.S. Data Privacy Framework and the European Commission's standard contractual clauses). Only if the company connects its own Stripe account. The Stripe account belongs to the company, and the company's own agreement with Stripe governs Stripe's processing; the platform only processes the copies.
- Visma e-conomic A/S (sub-processor): Bookkeeping data (the Bookkeeping module): entries and missing vouchers are fetched from the customer's e-conomic agreement. Location: Denmark (EU). Transfer: No transfer to third countries. Only if the company or its customer connects an e-conomic agreement. The agreement belongs to the customer; the platform fetches only what the automation uses.
- Erhvervsstyrelsen (CVR) (recipient of lookups): Lookup of company information by CVR number (KYC and customer creation). Location: Denmark (public authority). Transfer: No transfer to third countries. Only the CVR number (or a name) is sent in the lookup. The Danish Business Authority is a public authority, not a sub-processor; the lookup requires the company's own system-to-system access.
- cvrapi.dk (Online Gateway ApS, CVR 36421231) (recipient of lookups): Fallback lookup of public company data (name, address, industry) by CVR number or name. Location: Denmark. Transfer: No transfer to third countries. Only the CVR number or the searched name is sent; no information about persons is ever sent.

9. Transfers to third countries

Personal data is stored and processed in the EU/EEA by default. Transfers to a third country take place only through the sub-processors listed in section 8 and only on a valid transfer basis under GDPR Chapter V (the EU-U.S. Data Privacy Framework or the European Commission's standard contractual clauses with the necessary supplementary measures).

The processor does not otherwise transfer data to third countries on its own initiative and without instructions.

10. Assistance to the controller

Taking into account the nature of the processing and as far as possible through product features, the processor assists the controller in fulfilling its obligation to respond to requests for exercising the data subjects' rights (access,

rectification, erasure, restriction, data portability and objection): export per customer, anonymisation and deletion per customer, the customer portal where data subjects see and correct their own information, and the audit log.

The processor also assists the controller in ensuring compliance with GDPR Articles 32-36 (security, breach notification, impact assessments and prior consultation) with the information available to the processor.

The processor notifies the controller without undue delay and no later than 48 hours after becoming aware of a personal data breach affecting the company's data, with the information necessary for the controller to notify the Danish Data Protection Agency (Article 33) and the data subjects (Article 34). Notification is sent to the company's owner and administrators by email and in the system.

11. Audit and inspection

The processor makes available all information necessary to demonstrate compliance with GDPR Article 28 and this agreement, and allows for and contributes to audits, including inspections, conducted by the controller or an auditor mandated by the controller.

Audits are announced with at least 30 days' notice and carried out during normal working hours without undue disruption of operations, at most once a year unless there is a specific suspicion of a breach. The controller bears its own costs; the processor's reasonable costs of audits beyond the annual one may be invoiced by agreement. As documentation, the processor first makes available its description of security measures, sub-processor agreements and any independent audit reports.

12. Deletion and return on termination (annex D)

On termination the controller can export all its data itself (Settings ’ Data and test ’ export of all data and all files) and then delete the company in the system. Deleting the company removes all rows and files immediately; copies in backups are deleted as the backups expire.

If the controller has not deleted the company itself within 30 days after termination, the processor deletes the data after written notice to the company's owner, unless EU or national law requires continued storage.

The controller's own retention obligations (e.g. section 30 of the Danish anti-money laundering act on keeping customer due diligence information for 5 years after the end of the business relationship, and the bookkeeping act) rest with the controller, who must export the data before the company is deleted.

The processor confirms the deletion in writing on request.

13. Liability

The parties' liability follows GDPR Article 82 and the general rules of Danish law. The processor is liable for damage caused by processing where it has not complied with the obligations specifically directed at processors or has acted outside or contrary to the controller's lawful instructions.

14. Duration and termination

The agreement applies for as long as the processor processes personal data on behalf of the controller and cannot be terminated separately from the use of the service. It ends when the controller has deleted its company in the system, or when the processor has deleted the data under section 12.

If the agreement is amended, a new version with a new date is published in the system. The company's owner is asked to accept the new version; the previous version applies until the new one is accepted. If the company does not accept a new version, either party may terminate with 30 days' notice, and section 12 applies.

15. Acceptance

The agreement is accepted electronically by an owner of the company in the system (when the company is created, or under Settings ’ Company ’ Data processing agreement). The system records the agreement's version, the time, the accepting user's name and email and the IP address, and writes the acceptance to the company's audit log. The record is shown to the company's owner and administrators and can be downloaded as a PDF together with the text of the agreement.

Questions about the agreement should be sent to support@autora.nu.