

Data processing agreement

When you use FairSSL's services, FairSSL processes your domains, certificates and information about your servers on your behalf. This agreement describes how we do so. The page and PDF have the same content.

FairSSL's services, under GDPR Article 28

Version 1.1

Date 01-11-2026

Version 1.1, 01-11-2026.

The latest version is at fairssl.dk/en/data-processing-agreement/.

FairSSL A/S, CVR no. 33075782, Åbrovej 29, 8586 Ørum Djurs, Denmark

Contents

1. Parties
2. Services and purpose
3. Data subjects and personal data
4. The customer's instructions
5. FairSSL's obligations
6. Sub-processors
7. Transfers to countries outside the EU/EEA
8. Security measures
9. Security incidents
10. Assistance to the customer
11. Documentation and audit
12. Termination and deletion
13. Liability, changes and governing law

1. Parties

Processor: FairSSL A/S, CVR no. 33075782, Åbrovej 29, 8586 Ørum Djurs, Denmark, info@fairssl.dk ("FairSSL").

Controller: the customer using one of the services in section 2 ("the customer").

This agreement applies when the customer uses the services in section 2 and supplements FairSSL's terms of sale. In the event of a conflict, this agreement takes precedence over the terms of sale as regards the processing of personal data.

2. Services and purpose

This agreement covers the processing FairSSL carries out on the customer's behalf in these services:

- FairSSL ACME: the ACME server at fairssl.dk/acme, which the customer's own ACME clients use to order, renew and install certificates, including the information reported back by the installation script.
- Certificate monitoring: monitoring certificates and expiry on the servers and domains specified by the customer, monitoring Certificate Transparency logs (CT logs) for the customer's domains and sending alerts to the customer's contacts.
- TLS scanning: scanning the servers and ports specified by the customer, and the reports produced by the scans.
- API and control panel: the certificate and server information that the customer or the customer's systems submit to or retrieve from the API and control panel.

The sole purpose is to provide these services. FairSSL processes the customer's account, orders and billing as an independent controller; this is described in the privacy policy and is outside the scope of this agreement. This agreement applies for as long as FairSSL provides the services to the customer and thereafter until the data has been deleted under section 12.

3. Data subjects and personal data

Data subjects: the customer's employees and contacts who receive alerts or appear in certificates, ACME accounts and orders, and people whose name or email address forms part of a domain name or certificate.

Personal data, to the extent that the information can be linked to a person:

- Names and email addresses of contacts and alert recipients.
- Domain names and certificate information, including organisation name and address for OV and EV certificates.
- The ACME client's IP address and version in the event log.
- Server names, IP addresses and ports being monitored or scanned, and the monitoring and scan findings: certificate, expiry, protocols and errors.
- Certificates, CSRs and information about servers and installations that the customer submits to the control panel or through the API.
- Server name, thumbprint, result and error text from the installation, reported back by the installation script.

Special categories of personal data (GDPR Article 9) are not processed, and the customer must not enter them in names, descriptions or notes. With ACME, the customer's ACME client generates the private key, and FairSSL receives only the certificate signing request (CSR). If the customer uses FairSSL's CSR service, the private key is stored encrypted for no more than 60 days. Information in an issued certificate becomes public in CT logs.

4. The customer's instructions

FairSSL processes personal data only on the customer's documented instructions. These instructions consist of this agreement, the terms of sale, the customer's configuration and use of the services and anything else the parties agree in writing.

If FairSSL considers an instruction to infringe data protection rules, FairSSL informs the customer without undue delay. FairSSL does not use the data for its own purposes.

5. FairSSL's obligations

- Employees with access to the personal data are bound by confidentiality.
- FairSSL maintains the security measures described in section 8.
- FairSSL uses sub-processors only in accordance with section 6.
- FairSSL assists the customer with requests from data subjects and with the customer's obligations under GDPR Articles 32-36, as set out in section 10.
- FairSSL notifies the customer of security incidents in accordance with section 9.
- FairSSL deletes or returns the data on termination in accordance with section 12.
- FairSSL provides the customer with the information needed to demonstrate compliance with this agreement and GDPR Article 28, as set out in section 11.

6. Sub-processors

The customer gives FairSSL general authorisation to use sub-processors. The list of sub-processors, with country, purpose and status, is available at [fairssl.dk/en/sub-processors/](https://www.fairssl.dk/en/sub-processors/) and forms part of this agreement. Other suppliers do not process data on the customer's behalf and are listed in FairSSL's privacy policy.

FairSSL enters into a written agreement with each sub-processor imposing the same data protection obligations as this agreement, particularly regarding security measures. FairSSL is responsible to the customer for the sub-processor's processing.

Before a new sub-processor is used or an existing one is replaced, FairSSL gives notice by email to the customer's contacts and at [fairssl.dk/en/sub-processors/](https://www.fairssl.dk/en/sub-processors/), stating the date on which the change takes effect.

The customer may object to a new sub-processor within 30 days of the notice by writing to info@fairssl.dk. If the parties cannot find a solution, the customer may terminate the affected services without a minimum commitment period.

Sub-processors: <https://www.fairssl.dk/en/sub-processors/>

7. Transfers to countries outside the EU/EEA

If a sub-processor processes personal data outside the EU/EEA, it does so on a valid basis under GDPR Chapter V: an adequacy decision, including the EU-U.S. Data Privacy Framework, or the European Commission's standard contractual clauses. The basis for each supplier is stated in FairSSL's privacy policy and in the NIS2 and DORA documentation.

Certificate authorities (CAs) are not sub-processors. The CA for the selected product validates and issues the certificate as an independent controller under the CA/Browser Forum rules and may be established outside the EU, for example in the USA.

8. Security measures

FairSSL maintains technical and organisational measures appropriate to the risk, in accordance with GDPR Article 32. The main measures are:

- All traffic to the ACME server, control panel and API is encrypted with TLS 1.2 or later.
- The database and its backups are encrypted at rest, and the backups are stored in a different location from the database.
- Administrative access is limited to key personnel, with role-based access and the least privileges necessary.
- The customer can require two-factor authentication for all users of the account; an ACME account is created with a single-use EAB key.
- All changes go through version control, each deployment is traceable, and security updates are installed on an ongoing basis.
- [fairssl.dk](https://www.fairssl.dk) undergoes an external vulnerability scan weekly.
- Data minimisation: with ACME, FairSSL never holds the customer's private key.

FairSSL adjusts the measures when the risk or technology changes. FairSSL is not ISO 27001 certified; the controls are mapped to ISO/IEC 27001:2022 Annex A and CIS Controls v8.1, as described in the NIS2 and DORA documentation.

9. Security incidents

FairSSL notifies the customer without undue delay and within 48 hours at the latest if a security incident has affected the customer's data or the service. This also applies to a personal data breach at a sub-processor. A vulnerability that has been fixed without affecting the customer's data or the service is not an incident.

The notice includes, to the extent known: what happened, the categories and approximate number of data subjects and data records affected, the likely consequences, what FairSSL has done and will do, and whom the customer can contact. FairSSL assists the customer with notification to the supervisory authority and communication to the data subjects.

10. Assistance to the customer

FairSSL assists the customer in responding to requests from data subjects concerning their rights (GDPR Chapter III) and with the customer's obligations under GDPR Articles 32-36, taking into account the nature of the processing and the information available to FairSSL. If FairSSL receives a request directly from a data subject, FairSSL forwards it to the customer without undue delay.

FairSSL may charge for assistance beyond the capabilities of the services themselves, subject to prior agreement.

11. Documentation and audit

FairSSL makes available the information needed to demonstrate compliance with this agreement, including the NIS2 and DORA documentation, the sub-processor list and the latest scan report.

The customer may request an audit once a year and if a breach is suspected. The audit initially takes place through written documentation; an audit at FairSSL's premises is arranged with reasonable notice. The customer pays its own costs unless the audit reveals a material breach of this agreement. For large cloud providers, FairSSL relies on the provider's own certifications and attestations.

12. Termination and deletion

When FairSSL stops providing the services to the customer, or when the customer requests it, FairSSL deletes the personal data processed on the customer's behalf or returns it, at the customer's choice. Data is deleted from active systems within 30 days; backups are deleted when they expire in the ongoing rotation.

Data that FairSSL must retain under EU or Danish law, such as order and accounting data under the Danish Bookkeeping Act, is retained only for as long as the law requires. FairSSL cannot delete data that a CA must retain under the CA/Browser Forum rules or data in CT logs.

13. Liability, changes and governing law

The parties' liability under this agreement is subject to the limitation of liability in FairSSL's terms of sale, unless mandatory law provides otherwise.

FairSSL may update this agreement. A new version is published on this page with a new version number and date, and a change that restricts the customer's rights is notified by email at least 30 days before it takes effect.

This agreement is governed by Danish law. Disputes are settled by the Court of Randers (Retten i Randers).