

Databehandlersaftale

Når I bruger FairSSL's tjenester, behandler FairSSL jeres domæner, certifikater og oplysninger om jeres servere på jeres vegne. Aftalen beskriver, hvordan vi gør det. Siden og PDF'en har samme indhold.

FairSSL's tjenester, efter GDPR artikel 28

Version 1.1

Dato 01-11-2026

Version 1.1, 01-11-2026.

Den nyeste udgave ligger på fairssl.dk/da/databehandlersaftale/.

FairSSL A/S, CVR-nr. 33075782, Åbrovej 29, 8586 Ørum Djurs, Danmark

Indhold

1. Parter
2. Tjenester og formål
3. Registrerede og personoplysninger
4. Kundens instrukser
5. FairSSL's forpligtelser
6. Underdatabehandlere
7. Overførsel til lande uden for EU/EØS
8. Sikkerhedsforanstaltninger
9. Sikkerhedshændelser
10. Bistand til kunden
11. Dokumentation og audit
12. Ophør og sletning
13. Ansvar, ændringer og lovvalg

1. Parter

Databehandler: FairSSL A/S, CVR-nr. 33075782, Åbrovej 29, 8586 Ørum Djurs, Danmark, info@fairssl.dk (herefter "FairSSL").

Dataansvarlig: den kunde, der bruger en af tjenesterne i afsnit 2 (herefter "kunden").

Aftalen gælder, når kunden bruger tjenesterne i afsnit 2, og supplerer FairSSL's salgsbetingelser. Ved modstrid går denne aftale forud for salgsbetingelserne, for så vidt angår behandling af personoplysninger.

2. Tjenester og formål

Aftalen omfatter den behandling, FairSSL udfører på kundens vegne i disse tjenester:

- FairSSL ACME: ACME-serveren på fairssl.dk/acme, som kundens egne ACME-klienter bruger til at bestille, forny og installere certifikater, herunder de oplysninger, installationsscriptet melder tilbage.
- Certifikatovervågning: overvågning af certifikater og udløb på de servere og domæner, kunden angiver, overvågning af Certificate Transparency-logs (CT-logs) for kundens domæner og advarsler til kundens kontaktpersoner.
- TLS-scanning: scanning af de servere og porte, kunden angiver, og de rapporter, scanningen giver.
- API og kontrolpanel: de certifikat- og serveroplysninger, kunden eller kundens systemer lægger i eller henter fra API'et og kontrolpanelet.

Formålet er alene at levere disse tjenester. Kundens konto, ordrer og fakturering behandler FairSSL som selvstændig dataansvarlig; det er beskrevet i privatlivspolitikken og er ikke omfattet af denne aftale. Aftalen gælder, så længe FairSSL leverer tjenesterne til kunden, og derefter, indtil oplysningerne er slettet efter afsnit 12.

3. Registrerede og personoplysninger

Registrerede: kundens medarbejdere og kontaktpersoner, der modtager advarsler eller står i certifikater, ACME-konti og ordrer, og personer, hvis navn eller e-mailadresse indgår i et domænenavn eller et certifikat.

Personoplysninger, i det omfang oplysningerne kan knyttes til en person:

- Navn og e-mailadresse på kontaktpersoner og modtagere af advarsler.
- Domænenavne og certifikatoplysninger, for OV- og EV-certifikater også organisationsnavn og adresse.
- ACME-klientens IP-adresse og version i hændelsesloggen.
- Servernavne, IP-adresser og porte, der overvåges eller scannes, og hvad overvågningen og scanningen finder: certifikat, udløb, protokoller og fejl.
- Certifikater, CSR'er og oplysninger om servere og installationer, som kunden lægger i kontrolpanelet eller sender gennem API'et.
- Servernavn, thumbprint, resultat og fejlttekst fra installationen, som installationsscriptet melder tilbage.

Særlige kategorier af personoplysninger (GDPR artikel 9) behandles ikke, og kunden skal ikke skrive dem i navn, beskrivelser eller notater. Ved ACME laver kundens ACME-klient den private nøgle, og FairSSL modtager kun anmodningen om certifikatet (CSR). Bruger kunden FairSSL's CSR-service, gemmes den private nøgle krypteret i højst 60 dage. Oplysninger i et udstedt certifikat bliver offentlige i CT-logs.

4. Kundens instrukser

FairSSL behandler kun personoplysninger efter kundens dokumenterede instrukser. Instrukserne er denne aftale, salgsbetingelserne, kundens opsætning og brug af tjenesterne og det, parterne i øvrigt aftaler skriftligt.

Er en instruks efter FairSSL's vurdering i strid med databeskyttelsesreglerne, siger FairSSL det til kunden uden ugrundet ophold. FairSSL bruger ikke oplysningerne til egne formål.

5. FairSSL's forpligtelser

- Medarbejdere med adgang til personoplysningerne har tavshedspligt.

- FairSSL har de sikkerhedsforanstaltninger, afsnit 8 beskriver.
- FairSSL bruger kun underdatabehandlere efter afsnit 6.
- FairSSL hjælper kunden med anmodninger fra registrerede og med kundens forpligtelser efter GDPR artikel 32-36, jf. afsnit 10.
- FairSSL varsler kunden om sikkerhedshændelser efter afsnit 9.
- FairSSL sletter eller tilbageleverer oplysningerne ved ophør efter afsnit 12.
- FairSSL giver kunden de oplysninger, der skal til for at vise, at aftalen og GDPR artikel 28 overholdes, jf. afsnit 11.

6. Underdatabehandlere

Kunden giver FairSSL generel tilladelse til at bruge underdatabehandlere. Listen over dem, med land, formål og status, står på fairssl.dk/da/underleverandoerer/ og er en del af denne aftale. Andre leverandører behandler ikke data på kundens vegne og står i FairSSL's privatlivspolitik.

FairSSL indgår en skriftlig aftale med hver underdatabehandler, der pålægger den de samme databeskyttelsesforpligtelser som denne aftale, særligt om sikkerhedsforanstaltninger. FairSSL er over for kunden ansvarlig for underdatabehandlers behandling.

Før en ny underdatabehandler tages i brug eller en eksisterende udskiftes, varsler FairSSL det pr. mail til kundens kontaktpersoner og på fairssl.dk/da/underleverandoerer/ med den dato, ændringen gælder fra.

Kunden kan gøre indsigelse mod en ny underdatabehandler inden for 30 dage efter varslet ved at skrive til info@fairssl.dk. Finder parterne ikke en løsning, kan kunden opsige de berørte tjenester uden bindingsperiode.

Underdatabehandlere: <https://www.fairssl.dk/da/underleverandoerer/>

7. Overførsel til lande uden for EU/EØS

Behandles personoplysninger uden for EU/EØS hos en underdatabehandler, sker det på et gyldigt grundlag efter GDPR kapitel V: en afgørelse om tilstrækkeligt beskyttelsesniveau, herunder EU-U.S. Data Privacy Framework, eller EU-Kommissionens standardkontraktbestemmelser. Grundlaget for hver leverandør står i FairSSL's privatlivspolitik og i NIS2- og DORA-dokumentationen.

Certifikatudstederne (CA'erne) er ikke underdatabehandlere. Den CA, der hører til det valgte produkt, validerer og udsteder certifikatet som selvstændig dataansvarlig efter CA/Browser Forums regler og kan være etableret uden for EU, fx i USA.

8. Sikkerhedsforanstaltninger

FairSSL har tekniske og organisatoriske foranstaltninger, der passer til risikoen, jf. GDPR artikel 32. De vigtigste:

- Al trafik til ACME-serveren, kontrolpanelet og API'et er krypteret med TLS 1.2 eller nyere.
- Databasen og dens sikkerhedskopier er krypteret ved opbevaring, og sikkerhedskopierne ligger et andet sted end databasen.
- Administrativ adgang er begrænset til nøglepersoner med rollebaseret adgang og mindst mulige rettigheder.
- Kunden kan kræve to-faktor-login for alle kontoens brugere; en ACME-konto oprettes med en EAB-nøgle til engangsbrug.
- Alle ændringer sker gennem versionsstyring, hver udrulning er sporbar, og sikkerhedsopdateringer installeres løbende.
- fairssl.dk scannes ugentligt af en ekstern sårbarhedsscanning.
- Dataminimering: ved ACME har FairSSL aldrig kundens private nøgle.

FairSSL tilpasser foranstaltningerne, når risikoen eller teknikken ændrer sig. FairSSL er ikke certificeret efter ISO 27001; kontrollerne er kortlagt til ISO/IEC 27001:2022 bilag A og CIS Controls v8.1, som NIS2- og DORA-dokumentationen beskriver.

9. Sikkerhedshændelser

FairSSL varsler kunden uden unødigt forsinkelse og senest inden for 48 timer, hvis en sikkerhedshændelse har påvirket kundens data eller tjenesten. Det gælder også et brud på persondatasikkerheden hos en

underdatabehandler. En sårbarhed, der er lukket uden at have påvirket kundens data eller tjenesten, er ikke en hændelse.

Varslet indeholder, så vidt det vides: hvad der er sket, hvilke kategorier og omtrent hvor mange registrerede og oplysninger der er berørt, de sandsynlige konsekvenser, hvad FairSSL har gjort og vil gøre, og hvem kunden kan kontakte. FairSSL hjælper kunden med anmeldelsen til Datatilsynet og underretningen af de registrerede.

10. Bistand til kunden

FairSSL hjælper kunden med at besvare anmodninger fra registrerede om deres rettigheder (GDPR kapitel III) og med kundens forpligtelser efter GDPR artikel 32-36, under hensyn til behandlingens karakter og de oplysninger, FairSSL har. Modtager FairSSL en anmodning direkte fra en registreret, sender FairSSL den videre til kunden uden ugrundet ophold.

Bistand ud over det, tjenesterne selv kan, kan FairSSL fakturere efter forudgående aftale.

11. Dokumentation og audit

FairSSL stiller de oplysninger til rådighed, der skal til for at vise, at aftalen overholdes, herunder NIS2- og DORA-dokumentationen, underdatabehandlerlisten og den seneste scanningsrapport.

Kunden kan en gang om året, og ved mistanke om et brud, bede om en audit. Den sker først ved skriftlig dokumentation; en audit hos FairSSL aftales med rimeligt varsel. Kunden betaler sine egne omkostninger, medmindre auditten viser en væsentlig overtrædelse af aftalen. Hos store cloud-leverandører bygger FairSSL på leverandørens egne certificeringer og erklæringer.

12. Ophør og sletning

Når FairSSL holder op med at levere tjenesterne til kunden, eller når kunden beder om det, sletter FairSSL de personoplysninger, der er behandlet på kundens vegne, eller giver dem tilbage efter kundens valg. Sletning fra de aktive systemer sker inden for 30 dage; sikkerhedskopier slettes, når de udløber i den løbende rotation.

Oplysninger, som FairSSL skal opbevare efter EU-retten eller dansk ret, fx ordre- og regnskabsdata efter bogføringsloven, opbevares kun så længe, loven kræver. Det, en CA skal opbevare efter CA/Browser Forums regler, og det, der står i CT-logs, kan FairSSL ikke slette.

13. Ansvar, ændringer og lovvalg

Parternes ansvar efter aftalen følger ansvarsbegrænsningen i FairSSL's salgsbetingelser, medmindre ufravigelig lovgivning siger andet.

FairSSL kan opdatere aftalen. En ny version står på denne side med nyt versionsnummer og ny dato, og en ændring, der begrænser kundens rettigheder, varsles pr. mail mindst 30 dage før, den gælder.

Aftalen er underlagt dansk ret. Tvister afgøres ved Retten i Randers.