Personuppgiftsbiträdesavtal

När ni använder FairSSL:s tjänster behandlar FairSSL era domäner, certifikat och uppgifter om era servrar för er räkning. Avtalet beskriver hur vi gör det. Sidan och PDF:en har samma innehåll.

FairSSL:s tjänster, enligt GDPR artikel 28

Version 1.2
Datum 06-11-2026

Version 1.2, 06-11-2026.

Den senaste versionen finns på fairssl.se/sv/personuppgiftsbitradesavtal/.

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

Innehåll

1. Parter
2. Tjänster och ändamål
3. Registrerade och personuppgifter
4. Kundens instruktioner
5. FairSSL:s skyldigheter
6. Underbiträden
7. Överföring till länder utanför EU/EES
8. Säkerhetsåtgärder
9. Säkerhetsincidenter
10. Bistånd till kunden
11. Dokumentation och revision
12. Upphörande och radering
13. Ansvar, ändringar och lagval

1. Parter

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

Personuppgiftsansvarig: den kund som använder en av tjänsterna i avsnitt 2 (nedan "kunden").

Avtalet gäller när kunden använder tjänsterna i avsnitt 2 och kompletterar FairSSL:s försäljningsvillkor. Vid motstridighet har detta avtal företräde framför försäljningsvillkoren i fråga om behandling av personuppgifter.

2. Tjänster och ändamål

Avtalet omfattar den behandling som FairSSL utför för kundens räkning i dessa tjänster:

- FairSSL ACME: ACME-servern på fairssl.dk/acme, som kundens egna ACME-klienter använder för att beställa, förnya och installera certifikat, inklusive de uppgifter som installationsskriptet rapporterar tillbaka.
- Certifikatövervakning: övervakning av certifikat och utgångsdatum på de servrar och domäner som kunden anger, övervakning av Certificate Transparency-loggar (CT-loggar) för kundens domäner och varningar till kundens kontaktpersoner.
- TLS-skanning: skanning av de servrar och portar som kunden anger och de rapporter som skanningen ger.
- API och kontrollpanel: de certifikat- och serveruppgifter som kunden eller kundens system lägger in i eller hämtar från API:et och kontrollpanelen.

Ändamålet är enbart att leverera dessa tjänster. Kundens konto, beställningar och fakturering behandlar FairSSL som självständig personuppgiftsansvarig. Det beskrivs i integritetspolicyn och omfattas inte av detta avtal. Avtalet gäller så länge FairSSL levererar tjänsterna till kunden och därefter tills uppgifterna har raderats enligt avsnitt 12.

3. Registrerade och personuppgifter

Registrerade: kundens anställda och kontaktpersoner som tar emot varningar eller förekommer i certifikat, ACME-konton och beställningar, samt personer vars namn eller e-postadress ingår i ett domännamn eller ett certifikat.

Personuppgifter, i den mån uppgifterna kan knytas till en person:

- Namn och e-postadress till kontaktpersoner och mottagare av varningar.
- Domännamn och certifikatuppgifter, för OV- och EV-certifikat även organisationsnamn och adress.
- ACME-klientens IP-adress och version i händelseloggen.
- Servernamn, IP-adresser och portar som övervakas eller skannas samt vad övervakningen och skanningen hittar: certifikat, utgångsdatum, protokoll och fel.
- Certifikat, CSR:er och uppgifter om servrar och installationer som kunden lägger in i kontrollpanelen eller skickar via API:et.
- Servernamn, tumavtryck, resultat och feltext från installationen som installationsskriptet rapporterar tillbaka.

Särskilda kategorier av personuppgifter (GDPR artikel 9) behandlas inte, och kunden ska inte ange dem i namn, beskrivningar eller anteckningar. Vid ACME skapar kundens ACME-klient den privata nyckeln, och FairSSL tar endast emot certifikatbegäran (CSR). Om kunden använder FairSSL:s CSR-tjänst lagras den privata nyckeln krypterad i högst 60 dagar. Uppgifter i ett utfärdat certifikat blir offentliga i CT-loggar.

4. Kundens instruktioner

FairSSL behandlar endast personuppgifter enligt kundens dokumenterade instruktioner. Instruktionerna utgörs av detta avtal, försäljningsvillkoren, kundens konfiguration och användning av tjänsterna samt det som parterna i övrigt kommer överens om skriftligen.

Om FairSSL bedömer att en instruktion strider mot dataskyddsreglerna meddelar FairSSL kunden detta utan onödigt dröjsmål. FairSSL använder inte uppgifterna för egna ändamål.

5. FairSSL:s skyldigheter

- Anställda med tillgång till personuppgifterna omfattas av tystnadsplikt.
- FairSSL har de säkerhetsåtgärder som beskrivs i avsnitt 8.
- FairSSL använder endast underbiträden enligt avsnitt 6.
- FairSSL hjälper kunden med begäranden från registrerade och med kundens skyldigheter enligt GDPR artiklarna 32-36, enligt avsnitt 10.
- FairSSL underrättar kunden om säkerhetsincidenter enligt avsnitt 9.
- FairSSL raderar eller återlämnar uppgifterna när avtalet upphör enligt avsnitt 12.
- FairSSL ger kunden de uppgifter som behövs för att visa att avtalet och GDPR artikel 28 följs, enligt avsnitt 11.

6. Underbiträden

Kunden ger FairSSL ett allmänt tillstånd att anlita underbiträden. Förteckningen över dem, med ägarskap, var data lagras och ändamål, finns i avsnitt 3 i NIS2- och DORA-dokumentationen på fairssl.se/sv/nis2-dora/#underbitraden och utgör en del av detta avtal. Andra leverantörer behandlar inte data för kundens räkning och finns i FairSSL:s integritetspolicy.

FairSSL ingår ett skriftligt avtal med varje underbiträde som ålägger det samma dataskyddsskyldigheter som detta avtal, särskilt avseende säkerhetsåtgärder. FairSSL ansvarar gentemot kunden för underbiträdets behandling.

Innan ett nytt underbiträde anlitas eller ett befintligt ersätts meddelar FairSSL detta via e-post till kundens kontaktpersoner och i ändringsloggen på fairssl.se/sv/nis2-dora/#underbitraden, med det datum då ändringen börjar gälla.

Kunden kan invända mot ett nytt underbiträde inom 30 dagar från meddelandet genom att skriva till info@fairssl.dk. Om parterna inte hittar en lösning kan kunden säga upp de berörda tjänsterna utan bindningstid.

Underbiträden: https://www.fairssl.se/sv/nis2-dora/#underbitraden

7. Överföring till länder utanför EU/EES

Om personuppgifter behandlas utanför EU/EES hos ett underbiträde sker det på en giltig grund enligt GDPR kapitel V: ett beslut om adekvat skyddsnivå, inklusive EU-U.S. Data Privacy Framework, eller EU-kommissionens standardavtalsklausuler. Grunden för varje leverantör anges i FairSSL:s integritetspolicy och i NIS2- och DORA-dokumentationen.

Certifikatutfärdarna (CA:erna) är inte underbiträden. Den CA som hör till den valda produkten validerar och utfärdar certifikatet som självständig personuppgiftsansvarig enligt CA/Browser Forums regler och kan vara etablerad utanför EU, till exempel i USA.

8. Säkerhetsåtgärder

FairSSL har tekniska och organisatoriska åtgärder som är lämpliga för risken enligt GDPR artikel 32. De viktigaste är:

- All trafik till ACME-servern, kontrollpanelen och API:et krypteras med TLS 1.2 eller senare.
- Databasen och dess säkerhetskopior är krypterade vid lagring. Säkerhetskopior lagras alltid i ett eller flera EU-länder, åtskilda från det land där säkerhetskopian tas.
- Administrativ åtkomst är begränsad till nyckelpersoner med rollbaserad åtkomst och minsta nödvändiga behörighet.
- Kunden kan kräva tvåfaktorsautentisering för alla kontots användare. Ett ACME-konto skapas med en EAB-nyckel för engångsbruk.
- Alla ändringar görs genom versionshantering, varje driftsättning är spårbar och säkerhetsuppdateringar installeras löpande.
- fairssl.dk genomgår en extern sårbarhetsskanning varje vecka.
- Uppgiftsminimering: vid ACME har FairSSL aldrig kundens privata nyckel.

FairSSL anpassar åtgärderna när risken eller tekniken förändras. FairSSL är inte certifierat enligt ISO 27001. Kontrollerna är mappade mot ISO/IEC 27001:2022 bilaga A och CIS Controls v8.1, som beskrivs i NIS2- och DORA-dokumentationen.

9. Säkerhetsincidenter

FairSSL underrättar kunden utan onödigt dröjsmål och senast inom 48 timmar om en säkerhetsincident har påverkat kundens data eller tjänsten. Det gäller även en personuppgiftsincident hos ett underbiträde. En sårbarhet som har åtgärdats utan att påverka kundens data eller tjänsten är inte en incident.

Meddelandet innehåller, i den mån det är känt: vad som har hänt, vilka kategorier och ungefär hur många registrerade och personuppgiftsposter som berörs, de sannolika konsekvenserna, vad FairSSL har gjort och kommer att göra samt vem kunden kan kontakta. FairSSL hjälper kunden med anmälan till tillsynsmyndigheten och informationen till de registrerade.

10. Bistånd till kunden

FairSSL hjälper kunden att besvara begäranden från registrerade om deras rättigheter (GDPR kapitel III) och med kundens skyldigheter enligt GDPR artiklarna 32-36, med hänsyn till behandlingens art och de uppgifter som FairSSL har tillgång till. Om FairSSL får en begäran direkt från en registrerad vidarebefordrar FairSSL den till kunden utan onödigt dröjsmål.

FairSSL kan fakturera bistånd utöver det som tjänsterna själva kan utföra efter föregående överenskommelse.

11. Dokumentation och revision

FairSSL tillhandahåller de uppgifter som behövs för att visa att avtalet följs, inklusive NIS2- och DORA-dokumentationen, förteckningen över underbiträden och den senaste skanningsrapporten.

Kunden kan begära en revision en gång om året och vid misstanke om en överträdelse. Den sker först genom skriftlig dokumentation. En revision på plats hos FairSSL avtalas med rimligt varsel. Kunden betalar sina egna kostnader om revisionen inte visar en väsentlig överträdelse av avtalet. För stora molnleverantörer förlitar sig FairSSL på leverantörens egna certifieringar och intyg.

12. Upphörande och radering

När FairSSL slutar leverera tjänsterna till kunden, eller när kunden begär det, raderar FairSSL de personuppgifter som behandlats för kundens räkning eller återlämnar dem enligt kundens val. Radering från de aktiva systemen sker inom 30 dagar. Säkerhetskopior raderas när de löper ut i den löpande rotationen.

Uppgifter som FairSSL måste bevara enligt EU-rätt eller dansk rätt, till exempel beställnings- och bokföringsuppgifter enligt den danska bokföringslagen, bevaras endast så länge lagen kräver. FairSSL kan inte radera det som en CA måste bevara enligt CA/Browser Forums regler eller det som finns i CT-loggar.

13. Ansvar, ändringar och lagval

Parternas ansvar enligt avtalet följer ansvarsbegränsningen i FairSSL:s försäljningsvillkor om inte tvingande lagstiftning föreskriver annat.

FairSSL kan uppdatera avtalet. En ny version publiceras på denna sida med nytt versionsnummer och nytt datum. En ändring som begränsar kundens rättigheter meddelas via e-post minst 30 dagar innan den börjar gälla.

Avtalet omfattas av dansk rätt. Tvister avgörs av domstolen i Randers (Retten i Randers).