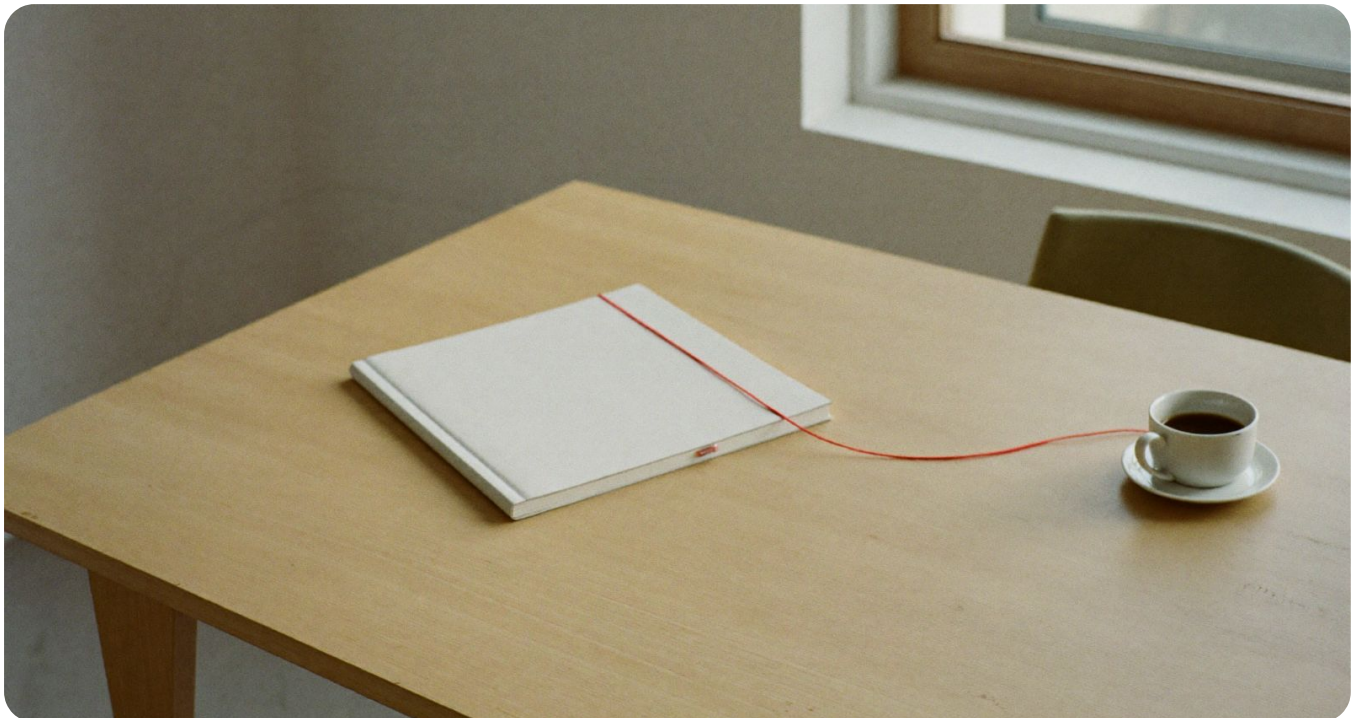


Din tryghed Udvidet rapport om data og sikkerhed i SPOR

Hvor data ligger, hvem der behandler dem, hvad SPOR aldrig må indeholde, hvordan SPOR er sat op, og status og bevis for hvert krav i GDPR, databeskyttelsesloven, AI-forordningen, ISO 27001-principperne, NIS2 og cookiereglerne.



Gennemgået
29. september 2026

Version
1.0

Kontakt
Martin Egesø · hey@martinegesoe.dk

1. Kort fortalt

Data i EU
Database og servere i Frankfurt. Mail fra Danmark.

AI kun i EU, på kundens egen konto
Låst i koden, i databasen og kontrolleret før hvert kald.

Ingen CPR-numre
Databasen afviser dem. Følsomme oplysninger (GDPR art. 9 og 10) må ikke lægges i SPOR.

Adskilt og beskyttet
Kundeadskillelse i databasen, obligatorisk tofaktor, kryptering, test før produktion.

16 af 24 krav er opfyldt med bevis.



SPOR er databehandler for de oplysninger, kunderne lægger i SPOR, og dataansvarlig for SPORs egne brugerkonti og logs.

2. Hosting og underleverandører

Leverandør og rolle	Placering	Data	Underdatabehandler og grundlag
Neon Inc. (PostgreSQL-database) Database. AI data i SPOR ligger her.	AWS eu-central-1, Frankfurt (EU)	Alle kundedata, brugerkonti, sessioner og logs. Krypteret under overførsel (TLS) og på disk (leverandørens kryptering).	Ja Data ligger i EU. Leverandøren er amerikansk og certificeret under EU-US Data Privacy Framework (Kommissionens tilstrækkelighedsafgørelse 2023/1795). Neons databehandleraftale indgår automatisk i vilkårene; kopi arkiveret i docs/juridisk/aftaler.
Vercel Inc. (hosting) Kører SPORs web- og serverfunktioner.	SPORs serverfunktioner kører i region fra1, Frankfurt (EU). Vercels driftslogs og kontodata kan behandles i USA.	Behandler forespørgsler undervejs i Frankfurt. Gemmer ikke kundedata; driftslogs indeholder adresse på siden, tidspunkt og IP-adresse.	Ja Vercel er certificeret under EU-US Data Privacy Framework (Kommissionens tilstrækkelighedsafgørelse 2023/1795). Vercels databehandlertillæg (vercel.com/legal/dpa) indgår automatisk i vilkårene, oplyser at den primære behandling sker i USA, og har EU's standardkontraktbestemmelser fra 2021 som reserve. Kopi arkiveret i docs/juridisk/aftaler.

Leverandør og rolle	Placering	Data	Underdatabehandler og grundlag
AWS Bedrock (Claude) på kundens egen AWS-konto AI til TheOffice og Laura, kun hvis kunden selv forbinder sin AWS-konto.	Kun EU: regionerne eu-central-1, eu-west-1, eu-west-3, eu-north-1 og kun modeller, der bliver i EU (ikke "us."/"global"-profiler). Låst i koden, i databasen og kontrolleret før hvert kald.	Kun det, kunden beder en AI-medarbejder om, og uddrag af kundens egne vejledninger. Hvert kald logges som dataoverførsel.	Nej Kundens egen aftale med AWS. SPOR sender kun, når kundens geografiske politik tillader regionen.
GitHub Inc. (kildekode og test) Kildekode, automatiske tests og udrulning.	USA	Ingen kundedata. Kun kode og testdata uden personoplysninger.	Nej Ikke relevant: ingen personoplysninger.
Simply.com (mail og DNS) Sender SPORs mails (invitationer, kundelinks, opstartsmails til nye kunder, driftsalarmer) via SMTP fra noreply@martinegesoe.dk; svar går til spor@martinegesoe.dk. Har også domænet og DNS for martinegesoe.dk. Hjemmesiden martinegesoe.dk ligger hos Vercel og er ikke en del af SPOR.	Danmark	Kun modtagerens e-mail og navn, afsender, arbejdspladsens eller kundens firmanavn og et link eller en liste over opstartstrin. Aldrig kundedata, adgangskoder, nøgler, svar, noter eller vedhæftninger. Sendes kun, når SMTP er sat op.	Ja Behandling i Danmark.

3. Data, som SPOR behandler

Oplysninger	Eksempler	Formål	Opbevaring
Brugerkonti og login	E-mail, adgangskode (kun som scrypt-hash), authenticator-hemmelighed (krypteret AES-256-GCM), gendannelseskoder (hash), sessioner (hash). IP-adresse kun som HMAC til begrænsning af loginforsøg.	Sikkert login med adgangskode og obligatorisk tofaktor.	Sessioner udløber efter 12 timer uden aktivitet og altid efter 7 dage. Kontoen findes, så længe brugeren har adgang.
Kundens registre og styring	Systemer, leverandører, AI-anvendelser, datakategorier (som betegnelser, fx "helbredsoplysninger", aldrig selve oplysningerne), beslutninger, dokumentation, opgaver, træning, vejledninger, kundeforløb og supportsager. Kan indeholde navne og arbejdsmails på ansvarlige og kontaktpersoner.	Kundens eget overblik over AI, data og ansvar.	Så længe kunden bruger SPOR. Slettes efter aftalt eksportperiode ved ophør (se exit-procedure).

Oplysninger	Eksempler	Formål	Opbevaring
Hændelser og brud	Beskrivelse af hændelsen, hvilke typer oplysninger der er berørt, vurdering og opfølgning. Hændelser med personoplysninger kan kun ses af indberetter, ansvarlig og ejer/administrator.	Dokumentation af hændelser og brud (fx 72-timers fristen).	Som kundens øvrige data; kunden kan sætte en historikperiode.
Hændelseslog	Hvem gjorde hvad hvornår, og hvilke data der blev sendt til hvilken udbyder og region.	Sporbarhed og dokumentation over for kunden og tilsyn.	Som kundens øvrige data; kunden kan sætte en historikperiode.
SPORs egne kunder (admin, kun operatør)	Firmanavn, CVR-nummer, kontaktperson og arbejdsmail, abonnement, fakturaer (beløb, datoer, status), tjekliste over kundens konti, opstartsliste, opgaver, sundhedstjek af kundens installation og en liste over systemer udviklet til kunden (hvor de ligger, AI-værktøjer og hvilke typer oplysninger de behandler, aldrig selve oplysningerne). Kundens egne data ligger på kundens egne konti, ikke her.	Kundeforhold, fakturering og drift. Kun SPOR-operatøren har adgang; databasen håndhæver det.	Så længe kundeforholdet består, og derefter efter bogføringslovens krav til regnskabsmateriale.
Offentligt indhold fra leverandører	Tekst fra leverandørers offentlige websider, hentet i AI Audit.	Vurdering af leverandørens AI-værktøj.	Som kundens øvrige data.

4. Data, som SPOR aldrig må indeholde

Oplysninger og regel	Kontrol	Håndhævelse
CPR-numre Databeskyttelsesloven § 11	Databasen afviser alt, der har form som et CPR-nummer, i alle kundetabeller, uanset hvor det kommer fra (formular, import, kundelink, support, AI-svar). Indhentede websider renses, før de gemmes. AI-svar med CPR-lignende tal gemmes ikke.	Afvises automatisk
Følsomme personoplysninger GDPR art. 9 (helbred, etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforening, genetiske og biometriske data, seksuelle forhold)	Må ikke lægges i SPOR. SPOR registrerer kun, AT en kunde behandler en type oplysninger, ikke selve oplysningerne. Reglen står ved de felter, hvor der skrives fritekst.	Regel i SPOR
Oplysninger om strafbare forhold GDPR art. 10 og databeskyttelsesloven § 8	Må ikke lægges i SPOR. Reglen står ved de felter, hvor der skrives fritekst.	Regel i SPOR

Oplysninger og regel	Kontrol	Håndhævelse
Kundens forretningsdata og kundernes kunders data GDPR art. 5, stk. 1, litra c (dataminimering)	SPOR har ingen forbindelser til kundens fagsystemer. Eneste undtagelse er kundens egen AI-konto og de vejledninger, kunden selv lægger ind.	Regel i SPOR
Betalingskortdata PCI DSS	SPOR modtager ikke betalinger og gemmer ingen kortdata.	Afvises automatisk

5. Regelgrundlag, status og bevis

Bevis er automatiske tests i SPORs kildekode, kontroller, der kører i den kørende SPOR efter hver udrulning, kode og aftaleudkast eller driftsdokumentation. De konkrete filer og kontroller fremgår af rapporten inde i SPOR (spor.martinegesoe.dk/tillid/rapport).

Databeskyttelsesforordningen (GDPR, EU 2016/679)

Gælder al behandling af personoplysninger i SPOR. Tilsyn: Datatilsynet.

Art. 5 og 25 Dataminimering og databeskyttelse gennem design Opfyldt

SPOR registrerer typer af oplysninger, ikke selve oplysningerne. CPR-numre afvises i databasen. Nye brugere får mindst mulige rettigheder, og roller styrer adgang.

Bevis: 2 automatiske tests · 1 live-kontrol · 1 i kode eller aftaleudkast

Art. 28 Databehandlersaftale med kunderne Delvist

SPOR er databehandler for kundens data. Aftalen skal beskrive formål, instruks, sikkerhed, underdatabehandlere og sletning. Indholdet til bilagene findes i denne dokumentation.

Mangler: Udkastet til databehandlersaftale og kundevilkår skal gennemgås juridisk og underskrives med hver kunde før rigtige kundedata.

Bevis: 2 i kode eller aftaleudkast

Art. 28, stk. 2 og 4 Underdatabehandlere Delvist

Neon (database) og Vercel (hosting) behandler kundedata for SPOR, begge i Frankfurt. Simply (Danmark) sender mails med modtagerens e-mail og et link. Listen står i denne rapport. AI kører på kundens egen konto.

Mangler: Aftalerne med Neon og Vercel er arkiveret. Simplys databehandlersaftale skal hentes i Simplys kontrolpanel og arkiveres.

Bevis: 2 live-kontroller · 1 i driftsdokumentationen

Art. 30, stk. 2 Fortegnelse som databehandler Opfyldt

Fortegnelsen ligger i admin (/admin/fortegnelse) og kan gemmes som PDF. Den rummer SPORs kontaktoplysninger, alle kunder (dataansvarlige) fra kunderegistret, kategorier af behandling, overførsler og sikkerhedsforanstaltninger. Indholdet hentes fra kunderegistret og fra denne dokumentation, så det altid er opdateret.

Bevis: 1 automatisk test · 3 i kode eller aftaleudkast

Art. 32 **Behandlingssikkerhed** Opfyldt

Kundeadskillelse i databasen (Row-Level Security, tvunget), login med adgangskode og obligatorisk tofaktor, kryptering under overførsel (TLS) og af hemmeligheder (AES-256-GCM), app-rollen kan ikke omgå adskillelsen, Content Security Policy, fuld hændelseslog.

Bevis: 3 automatiske tests · 4 live-kontroller

Art. 32, stk. 1, litra c **Gendannelse efter hændelser** Delvist

Neon tager løbende backup (point-in-time restore). Fremgangsmåden står i driftshåndbogen og sikrer, at slettede data ikke genopstår; en kontrol af den gendannede database er bygget.

Mangler: Neons historikvindue er i dag 1 dag; overvej 7 dage. Gennemfør første gendannelsesøvelse.

Bevis: 1 automatisk test · 1 i driftsdokumentationen

Art. 33 og 34 **Håndtering af brud** Opfyldt

Procedure for brud i SPOR selv (underretning af kunder uden unødigt forsinkelse; anmeldelse inden 72 timer for SPORs egne konti). Kundernes egne brud registreres i SPORs hændelsesmodul med 72-timers frist.

Bevis: 1 automatisk test · 1 i driftsdokumentationen

Art. 44-46 **Overførsel til tredjelande** Delvist

Kundedata opbevares og behandles i EU (database og servere i Frankfurt, mail i Danmark). Vercels tekniske driftslogs (IP-adresse, sideadresse, tidspunkt) kan behandles i USA; Vercel og Neon er certificeret under EU-US Data Privacy Framework. AI kan kun kaldes i EU-regioner med modeller, der bliver i EU; det er låst i koden, i databasen og kontrolleres før hvert kald. Hver dataoverførsel logges.

Mangler: Grundlaget er dokumenteret for Neon og Vercel (Data Privacy Framework, standardkontraktbestemmelser som reserve). Følg sagen om Data Privacy Framework ved EU-Domstolen; falder den, gælder standardkontraktbestemmelserne, og en vurdering af overførslen skal laves.

Bevis: 2 automatiske tests · 4 live-kontroller

Art. 9 og 10 **Ingen følsomme oplysninger eller strafbare forhold** Opfyldt

Må ikke lægges i SPOR. Reglen står ved fritekstfelterne. SPOR registrerer kun typer af oplysninger.

Bevis: 1 i kode eller aftaleudkast

Art. 15-20 og 28, stk. 3, litra g **Indsigt, eksport og sletning** Opfyldt

Kunden kan eksportere alle sine data (JSON og CSV) uden hemmeligheder. Ved ophør bliver arbejdspladsen skrivebeskyttet, forbindelser, agenter og links lukkes, og data slettes efter eksportperioden.

Bevis: 2 automatiske tests · 1 i driftsdokumentationen

Art. 13 **Oplysning til brugerne** Delvist

Privatlivspolitikken for SPOR er udgivet på spor.martinegesoe.dk/privatliv og linket fra login, sidehovedet og menuen. Den skelner mellem kundens data (kunden er dataansvarlig) og SPORs egne brugerkonti, logs og kundeadministration. Hjemmesiden martinegesoe.dk har sin egen politik for henvendelser og kunder.

Mangler: Privatlivspolitikkerne (SPOR og martinegesoe.dk) skal gennemgås juridisk.

Bevis: 3 i kode eller aftaleudkast

Databeskyttelsesloven (DK)

Danske særregler, bl.a. om CPR-numre. Tilsyn: Datatilsynet.

§ 11 Ingen CPR-numre Opfyldt

Databasen afviser CPR-numre i alle kundetabeller, uanset kilde. En test fejler, hvis en ny tabel mangler spærren, og driftstjekket viser det live.

Bevis: 1 automatisk test · 1 live-kontrol · 1 i kode eller aftaleudkast

AI-forordningen (EU 2024/1689)

SPOR bruger AI som værktøj for kunden og hjælper kunderne med deres egne pligter. Tilsyn: Digitaliseringsstyrelsen (dansk koordinerende myndighed).

Art. 50 Tydeligt, når man arbejder med AI Opfyldt

AI-medarbejdere i TheOffice er tydeligt markeret som software. AI-forslag skal godkendes af et menneske, før de bliver til handlinger.

Bevis: 2 automatiske tests

Art. 6 og bilag III SPORs egen brug af AI er ikke højrisiko Opfyldt

AI i SPOR udarbejder udkast og svar ud fra kundens egne kilder. Den træffer ikke afgørelser om personer og indgår ikke i bilag III-områder.

Bevis: 1 i kode eller aftaleudkast

Art. 4 AI-kundskaber Opfyldt

SPOR har træningsmoduler og vejledninger, så kunderne kan dokumentere medarbejdernes AI-kundskaber.

Bevis: 1 automatisk test

Informationssikkerhed efter ISO/IEC 27001-principperne

SPOR er ikke certificeret. Kontrollerne er dokumenteret, så en offentlig kunde kan vurdere SPOR som leverandør. Tilsyn: Digitaliseringsstyrelsen kræver ISO 27001 af statslige myndigheder.

A.5.15-5.18, A.8.5 Adgangsstyring og stærk autentifikation Opfyldt

Ingen offentlig tilmelding. Adgangskode og obligatorisk tofaktor for alle. Roller pr. arbejdsplads. Supportadgang kun tidsbegrænset og logget.

Bevis: 2 automatiske tests

A.8.15 Logning Opfyldt

Alle ændringer, loginhændelser og dataoverførsler logges pr. kunde. Et dagligt tjek overvåger installationer og sender én samlet alarm.

Bevis: 2 automatiske tests

A.5.19-5.22 **Leverandørstyring** Delvist

Få leverandører, alle listet med placering og rolle. Nye afhængigheder kan ikke tilføjes, uden at dokumentationen opdateres (automatisk test).

Mangler: Arkivér Simplys databehandleraftale (Neon og Vercel er arkiveret).

Bevis: 1 automatisk test

A.8.32 **Ændringsstyring** Opfyldt

AI kode går gennem GitHub med automatiske tests. Ændringer afprøves først i et separat testmiljø (dev.spor.martinegesoe.dk) med sin egen database uden kundedata, før de godkendes til produktion. Udrulning sker kun efter grønne tests og kørte databasemigrationer; bagefter kontrolleres, at den nye version kører, og at test og produktion ikke deler database.

Bevis: 1 automatisk test · 2 live-kontroller · 1 i kode eller aftaleudkast

A.8.24 **Kryptering** Opfyldt

TLS på alle forbindelser. Hemmeligheder krypteres med AES-256-GCM. Adgangskoder gemmes som script-hash.

Bevis: 1 automatisk test · 2 live-kontroller

A.8.26 **Beskyttelse af webapplikationen** Delvist

Content Security Policy med nonce pr. forespørgsel, ingen eksterne scripts, beskyttede cookies (__Host-, httpOnly, secure), AI Audit kan ikke kalde interne adresser.

Mangler: Politikken er afprøvet håndhævet på de offentlige sider uden overtrædelser. Sæt SPOR_CSP=enforce i testmiljøet, gennemgå de indloggede sider der, og sæt den derefter i produktion.

Bevis: 2 automatiske tests · 1 live-kontrol

A.8.24 **Nøgleskift** Opfyldt

Krypteringsnøglen opbevares i Vercel og et sikkert sted uden for Vercel. Nøgleskift sker med genkryptering af alle hemmeligheder (npm run datakey:rotate), mens den forrige nøgle stadig kan læse.

Bevis: 1 automatisk test · 1 i driftsdokumentationen

NIS2 (EU 2022/2555) og den danske NIS2-lov

Cybersikkerhed for væsentlige og vigtige enheder. Tilsyn: Styrelsen for Samfundssikkerhed m.fl.

Art. 2-3 **Omfattet eller ej** Delvist

MLE Gruppo ApS er under størrelsesgrænsen for væsentlige og vigtige enheder. SPOR følger alligevel de samme grundprincipper (risikostyring, hændelseshåndtering, leverandørstyring, kryptering, adgangsstyring).

Mangler: Vurderingen af, at virksomheden ikke er omfattet, skal bekræftes af juridisk rådgiver og genbesøges ved vækst.

Bevis: 1 i driftsdokumentationen

Cookiebekendtgørelsen

Samtykke til cookies, der ikke er strengt nødvendige. Tilsyn: Digitaliseringsstyrelsen.

§ 3 Kun nødvendige cookies Opfyldt

SPOR sætter kun login-cookies, der er strengt nødvendige. Ingen statistik, reklame eller sporing, og ingen tredjepartsscripts. Derfor kræves der ikke samtykke.

Bevis: 1 automatisk test · 1 i kode eller aftaleudkast

6. Åbne punkter

- **Databehandleraftale med kunderne** Delvist
Udkastet til databehandleraftale og kundevilkår skal gennemgås juridisk og underskrives med hver kunde før rigtige kundedata.
- **Underdatabehandlere** Delvist
Aftalerne med Neon og Vercel er arkiveret. Simplys databehandleraftale skal hentes i Simplys kontrolpanel og arkiveres.
- **Gendannelse efter hændelser** Delvist
Neons historikvindue er i dag 1 dag; overvej 7 dage. Gennemfør første gendannelsesøvelse.
- **Overførsel til tredjelande** Delvist
Grundlaget er dokumenteret for Neon og Vercel (Data Privacy Framework, standardkontraktbestemmelser som reserve). Følg sagen om Data Privacy Framework ved EU-Domstolen; falder den, gælder standardkontraktbestemmelserne, og en vurdering af overførslen skal laves.
- **Oplysning til brugerne** Delvist
Privatlivspolitikkerne (SPOR og martinegesoe.dk) skal gennemgås juridisk.
- **Leverandørstyring** Delvist
Arkivér Simplys databehandleraftale (Neon og Vercel er arkiveret).
- **Beskyttelse af webapplikationen** Delvist
Politikken er afprøvet håndhævet på de offentlige sider uden overtrædelser. Sæt SPOR_CSP=enforce i testmiljøet, gennemgå de indloggede sider der, og sæt den derefter i produktion.
- **Omfattet eller ej** Delvist
Vurderingen af, at virksomheden ikke er omfattet, skal bekræftes af juridisk rådgiver og genbesøges ved vækst.

SPOR er ikke certificeret, og denne rapport er ikke en garanti for, at alle krav er opfyldt. Den viser status og bevis pr. 29. september 2026. Kundens egen efterlevelse afhænger også af kundens anvendelse og beslutninger. Rapporten bygges automatisk ud fra SPORs dokumentation og opdateres, når SPOR ændres.