FINANSMINISTERIET

Tilsyn med SAMs rolle som databehandler

TR 3/2025 - it-tilsyn - December 2025

Indhold

Tilsynsrapport om tilsyn med SAM' rolle som databehandler
TR 3/2025

Denne tilsynsrapport er udarbejdet af:
CTJ/MRA
19-12-2025

Tilsynsrapporten er sendt til:
Att.: Økonomistyrelsen Direktør Line Nørbæk
Statens Administration Direktør Trine Nielsen

1. Konklusion

Center for Tilsyn og Jura (herefter CTJ) i Finansministeriets departement har i november 2025 afsluttet vores tilsyn med Statens Administration (herefter SAM) som databehandler for 2025. Tilsynet med SAM omfatter de forpligtelser, der påhviler SAM som databehandler i henhold til databeskyttelsesforordningen (GDPR).

Overordnet konkluderer CTJ således:

Tabel 1
Overordnet konklusion

Vurderingsgrundlag	Samlet modenhedsvurdering
Basal beskyttelse	Høj beskyttelse
Den basale beskyttelse sikrer, at kravene i GDPR er opfyldt. Tilsynet har fokus på: • Intern regulering (krav til databehandlere), jf. afsnit 3.2.1. • Databehandleraftaler (krav til databehandleraftalen), jf. afsnit 3.2.2. • Fortegnelse (krav til indholdet af databehandlerens fortegnelse), jf. afsnit 3.2.3. • Oplysning (kontrol med databehandleren - tilsyn), jf. afsnit 3.3.	
Effektiv beskyttelse	Effektiv beskyttelse
Den effektive beskyttelse sikrer en databeskyttelse gennem: • Internt regelsæt (politikker og procedurer), jf. afsnit 3.2. • Et ledelsessystem (Anneks A i ISO 27001), jf. afsnit 3.2.4. • Risikovurdering og -styring (risikobaseret tilgang til behandlingssikkerhed - passende sikkerhedsniveau), jf. afsnit 3.2.4. • Dokumentation (påvise/dokumentere overholdelse af GDPR krav), jf. afsnit 3.2.	

På vegne af den dataansvarlige (herefter kunden) foretager SAM behandling af personoplysninger. Dette gøres i praksis ved at etablere en databehandleraftale, som både kunden og SAM underskriver. I aftalen er det klarlagt, hvordan data skal behandles.

Det udførte tilsyn med den basale beskyttelse har vist, at SAM efterlever de krav, der er fastsat i artikel 28. Her er det blandet andet fastlagt, at SAM kun behandler personoplysninger efter instruks fra kunden, herunder hvorvidt SAM kan overføre personoplysninger til et tredjeland eller en international organisation, og at SAM iværksætter passende foranstaltninger og underretter kunden ved konstatering af brud på persondatasikkerheden, samt om ikke at anvende en underdatabehandler uden forudgående godkendelse.

SAM skal i henhold til databehandleraftalen bistå med at tilvejebringe de informationer, som angivet i bestemmelse 10.3 og nærmere beskrevet i forordningens artikel 33, stk. 3. I relation hertil har SAM indtil december 2025 underrettet kunderne ved konstatering af 81 brud på persondatasikkerheden. Det er lidt flere brud i forhold til samme periode i 2024. SAM træffer løbende beslutning om awareness, tiltag eller andre initiativer med henblik på at nedbringe antallet af anmeldte brud.

SAM skal som minimum gennemføre 10 tekniske og obligatoriske foranstaltninger, som er aftalt med kunden i den indgående databehandleraftale. Foranstaltningerne er gennemført ved etablering af de tekniske foranstaltninger og den løbende informationssikkerhedsstyring i SAM. I en tabel har CTJ foretaget en præcisering af, hvordan krav til de gennemførte foranstaltninger er opfyldt.

2. Formål og omfang

CTJ i Finansministeriets departement fører tilsyn med informationssikkerheden i SAM. Tilsynet er baseret på det fællesstatslige tilsynskoncept, som er obligatorisk og beskriver departementets overordnede tilsynsansvar.

Formålet med dette tilsyn er at dække kundens behov for indsigt i og sikring af SAM's betryggende behandling af personoplysninger som databehandler. CTJ's tilsynsmodel er anvendt til at vurdere modenheden og effektiviteten i forhold til at efterleve de relevante databeskyttelsesretlige regler.

I GDPR stilles der krav om, at databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i artikel 28, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner og inspektioner.

I databehandleraftalens afsnit 12 om Revision, herunder inspektion, er kundens tilsyn med SAM som databehandler beskrevet og gengivet nedenfor.

"Finansministeriets departement fører tilsyn med Statens Administration som databehandler på vegne af alle kunder, jf. databeskyttelsesforordningens art. 28, stk. 3, litra h. Finansministeriets departement afgiver årligt en tilsynsrapport vedrørende Statens Administration som databehandler. Desuden skal databehandleren i den forbindelse, og hvis det skønnes nødvendigt for den dataansvarlige, give mulighed for og bidrage til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller af en revisor, som er bemyndiget hertil af den dataansvarlige".

Det enkelte tilsyn har til formål at konkludere og rapportere til ledelsen på resultatet af det gennemførte tilsyn. Udkast til en tilsynsrapport forelægges for SAM' daglige ledelse og endelig tilsynsrapport for topledelsen i SAM.

For at imødegå kundens krav om egen tilsyn eller revision varetages tilsynet med SAM som databehandler af CTJ. Tilsynet skal give kunden information om, hvorvidt SAM beskytter og behandler data, som foreskrevet i GDPR. Der henvises til Datatilsynets vejledning om tilsyn med databehandlere, hvor koncept 5 giver enten en myndighed mulighed for at føre tilsyn på vegne af flere myndigheder eller en uafhængig tredjepart til at udføre et tilsyn på vegne af alle de dataansvarlige. Via denne tilsynsrapport kan kunden eventuel få indtryk af observationer hos SAM.

3. Resultat

3.1 Det overordnede grundlag

Behandling af personoplysninger aftales i en databehandleraftale mellem kunden og SAM.

Som følge af ressortoverførsel af en række administrative opgaver inden for løn, personale, bogholderi og regnskab ved kongelig resolution behandler SAM som databehandler personoplysninger på kundens vegne, og hermed skal SAM også opfylde GDPR krav til behandling og sikkerhed. Kunden har fortsat ansvaret som dataansvarlig, og dette ansvar overgår således ikke til SAM ved ressortoverførslen.

CTJ' tilsyn med SAM som databehandler udføres med fremsendelse af en spørgeramme med deadline for aflevering af svar og materiale i Q4. Materialet drøftes og vurderes. SAM inddrages løbende i processen og i høringen af tilsynsrapport.

3.2 Etablering af dokumentation

Med baggrund i CTJ's vurderinger foretages en bedømmelse af de enkelte kontrolmål. Det vurderes i tilsynet, om SAM kan dokumentere:

- opfyldelse af krav i GDPR og
- effektiv behandling af personoplysninger i henhold til databehandleraftalen med tilhørende instruks fra kunden.

Tabel 2
Artikler og kontrolmål, som er databehandlerens ansvar

Artikel	Kontrolmål	Vurdering
28 og 29	Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale.	
30,2	Der efterleves procedurer og kontroller, som sikrer, at databehandleren fører en fortegnelse over kategorier af behandlinger, der foretages på vegne af den dataansvarlige.	
32	Der efterleves procedurer og kontroller, som sikrer, at databehanderen har implementeret tekniske og organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.	
33,2	Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.	
35 og 28.3f	Der efterleves procedurer og kontroller, som sikrer, at databehandleren bistår den dataansvarliges forpligtelse til at gennemføre en konsekvensanalyse vedr. databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.	
36 og 28.3f	Der efterleves procedurer og kontroller, som sikrer, at databehandleren bistår den dataansvarliges forpligtelse til at høre tilsynsmyndigheden inden behandling, såfremt en konsekvensanalyse vedr. databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.	

Bedømt ved grønt trafiklys – opfyldt/effektivt, gult trafiklys – ikke helt opfyldt/effektivt og rødt trafiklys – ikke opfyldt/effektivt.
Inspiration fra ISAE 3000-erklæring, som giver sikkerhed for, at databehandlere lever op til kravene i GDPR, som de har forpligtet sig til i de indgåede databehandleraftaler.

3.2.1 Krav til databehandlere (artikel 28, stk. 1)

I henhold til kongelig resolution overlader kunden behandling af personoplysninger til SAM. Kunden skal sikre sig, at SAM har de nødvendige tekniske og organisatoriske foranstaltninger på plads. Opgaven, der udføres af SAM, skal være reguleret i en skriftlig, herunder elektronisk, databehandleraftale, som skal beskrive opgaven og kundens rolle.

SAM anvender en enslydende standard databehandleraftale, som reguleres løbende med ændringer fra Datatilsynets skabelon og selv udført af SAM. Den seneste version 1.2 af aftalen er fra juli 2023. I 2024 forelå der aftaler med alle kunder i SAM.

SAM har i juni 2025 foretaget en vurdering af standard databehandleraftaler (skabelon) med kunder og leverandører, og disse aftaler er ajourført. Vurderingen har ikke givet anledning til nye opdateringer. SAM har bekræftet, at de fortsat anvender versionen fra juli 2023.

3.2.2 Krav til databehandleraftalen (artikel 28, stk. 3)

Databehandleraftalen skal regulere forholdene hos SAM og beskrive dennes forpligtelser i relation til databehandlingen. Disse forpligtelser (eller minimumskrav til aftalen) er omtalt i tabel 3 og efterfølgende præciseret.

Tabel 3
Minimumskrav

Artikel	Forpligtelse	Udførte test	Vurdering
28,3 a	Behandle og overføre personoplysninger efter dokumen-teret instruks.	Påset at der foreligger en skriftlig instruks i form af bilag til databehandleraftalen. Sikring af, at kundens instruks om behandling af personoplysninger overholdes, foretages i revision/tilsyn af Regnskab, Løn og Refusion (jf. bilag A). Efterlevelse af databehandleraftalens forpligtelser foretages her i tilsynsrapporten (jf. bilag C).	
28,3 b	Personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller underlagt en passende lovbestemt tavshedspligt.	Offentlige ansatte er underlagt tavshedspligt (jf. forvaltningsloven).	I/A
28,3 c	Iværksætte alle foranstaltninger, som kræves iht. A 32 om behandlingssikkerhed.	Vunderet, jf. A 32-foranstaltninger (jf. 3.2.4).	
28,3 d	Opfylde de betingelser, der er omhandlet i stk. 2 og 4, for at gøre brug af underdatabehandler.	Påset, at der foreligger en skriftlig instruks i form af bilag (underleverandører) til databehandleraftalen. Test af, at SAM har sikret, at der stilles de fornødne garantier for, at partnere vil gennemføre passende foranstaltninger på en sådan måde, at behandlingen opfylder kravene i forordningen.	
28,3 e	Bistå kunden ved hjælp af passende tekniske og organisatoriske foranstaltninger og med opfyldelse af kundens forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder.	Påset, at der foreligger en skriftlig procedure, som beskriver, hvordan SAM bistår kunden med opfyldelse af kundens forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder som fastlagt i forordningens kapitel III.	
28,3 f	Bistå kunden med at sikre overholdelse af forpligtelserne efter artikel 32-36.	Vurderet, der omfatter bistand til A 32-foranstaltninger. A 33,2-underretning om brud. A 35/36-konsekvensanalyse og forudgående høring.af DT	
28,3 g	Slette eller tilbagelevere alle personoplysninger til den dataansvarlige, efter behandlingen er ophørt.	Påset ,at der foreligger en skriftlig procedure, som beskriver, hvordan SAM efter kundens valg sletter eller tilbageleverer alle personoplysninger.	
28,3 h	Stille alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i A 28 til rådighed for kunden samt giver mulighed for og bidrager til revisioner mv.	Afrapporteret resultatet af det gennemførte tilsyn i en tilsynsrapport. SAM lægger rapporten på hjemmesiden.	I/A

Anm.: Vurdering omfatter en kravsopfyldelse og effektivitet.Trafiklys grøn, gul og rød anvendes.

Ad a) Databehandleraftalen i medfør af litra a
Aftalens bestemmelse 4, Databehandleren handler efter instruks, er i overensstemmelse med artikel 28, stk. 3a.

SAM må kun behandle personoplysninger efter dokumenteret instruks fra kunden, herunder overførsel af personoplysninger til et tredjeland. For så vidt angår overførsel af personoplysninger til et tredjeland henvises der til databehandleraftalens bestemmelse 8 om overførsel til tredjelande eller internationale organisationer. Hvis en overførsel af personoplysninger skal finde sted i forbindelse med brugen af databehandler i et tredjeland, angives dette i bilag C.6.

Kravet om, at instruksen skal være dokumenteret, må antages at bestå i, at såvel kunden som SAM kan dokumentere instruksen, så begge parter kan sikre sig, at forordningens regler efterleves ved den konkrete behandling af personoplysninger.

Databehandleraftalens bilag A og C udgør instruksen til behandlingen, som omfatter administrativ sagsbehandling herunder indsamling, registrering, brug og opbevaring af personoplysninger.

Hvor det er relevant, skal SAM i fortegnelsen (jf. afsnit 3.2.3) oplyse om overførsler af personoplysninger til et tredjeland eller en international organisation. Fortegnelsen indeholder ikke oplysning om tredjelandsoverførsler.

Ad b) Databehandleraftalen i medfør af litra b
Aftalens bestemmelse 5. Fortrolighed er i overensstemmelse med artikel 28, stk. 3b.

SAM skal sikre, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

SAM må kun give adgang til personoplysninger, som behandles på kundens vegne, til personer, som underlagt SAM' instruktionsbeføjelser. Listen af personer, som har fået tildelt adgang til personoplysninger, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.

Den periodiske gennemgang af tildelte brugeradgangsrettigheder er omfattet af SAM's almindelige processer for adgangsstyring.

Det må antages, at forpligtelsen er opfyldt for offentlige myndigheder, der fungerer som databehandlere, idet offentligt ansatte er underlagt tavshedspligt, jf. forvaltningslovens § 27, stk. 1.

Ad c) Databehandleraftalen i medfør af litra c
Aftalens bestemmelse 6 om Behandlingssikkerhed er i overensstemmelse med artikel 28, stk. 3c.

SAM skal iværksætte alle foranstaltninger, som kræves i henhold til artikel 32 om behandlingssikkerhed. Der henvises til afsnit 3.2.4 om behandlingssikkerhed.

Ad d) Databehandleraftalen i medfør af litra d
Aftalens bestemmelse 7 om Anvendelse af underdatabehandlere er i overensstemmelse med artikel 28, stk. 3d.

Det skal fremgå af aftalen, at databehandleren skal opfylde de betingelser, der er omhandlet i stk. 2 og 4, for at gøre brug af en underdatabehandleraftale.

Brug af underdatabehandler, som varetager noget af databehandlingen for SAM, kan enten ske ved specifik eller generel skriftlig godkendelse fra kunden. De konkret anvendte underdatabehandlere fremgår af bilag B.

SAM har i en vejledning for leverandørstyring beskrevet, hvordan leverandørstyringen håndteres i SAM med fokus på kategorisering af leverandør samt revision og tilsyn af leverandører.

På baggrund af leverandørtilsynsnotat med SIT, hvor SAM' tilsyn har taget udgangspunkt i leverandørkategorisering af SIT, Beretning om tilsynet med SIT og tilsynsrapport med SIT' rolle som databehandler, vurderer SAM, at de leverancer/services, SAM modtager fra SIT, er på et tilfredsstillende niveau jævnfør indgåede kundeaftale og databehandleraftale.

SAM har i en vejledning for indgåelse af databehandleraftale med leverandører beskrevet procedure og regelsæt for indgåelse af databehandleraftaler med leverandører i SAM.

Ad e-f) Databehandleraftalen i medfør af litra e og f
Aftalens bestemmelse 9 om Bistand til den dataansvarlige er i overensstemmelse med artikel 28, stk. 3e-f.

SAM skal under hensyntagen til behandlingens karakter så vidt muligt bistå kunden ved hjælp af passende tekniske og organisatoriske foranstaltninger og med opfyldelse af kundens forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder, som fastlagt i forordningens kapitel III. Registrerede kan ikke udøve deres rettigheder direkte over for SAM, men kunden kan være afhængig af SAM's bistand ved opfyldelse af de registreredes rettigheder. Desuden skal SAM bistå kunden

med at sikre overholdelse af forpligtelserne efter artikel 32-36 under hensyn til behandlingens karakter og de oplysninger, der er tilgængelige for SAM.

Der henvises til rapportens afsnit om de ovennævnte artikler. SAM skal således bistå kunden med behandlingssikkerhed efter artikel 32, men også med at anmelde brud på persondatasikkerheden til Datatilsynet efter artikel 33 og med at foretage underretning om brud på persondatasikkerheden i forhold til de registrerede i medfør af artikel 34. Endvidere skal SAM bistå kunden med at udarbejde konsekvensanalyser vedrørende databeskyttelse i medfør af artikel 35 samt foretage forudgående høring af Datatilsynet, såfremt en konsekvensanalyse viser, at den pågældende behandling vil føre til høj risiko, jf. artikel 36.

SAM har beskrevet regelsæt for håndtering af henvendelser vedrørende GDPR i en vejledning om håndtering af henvendelser i relation til databeskyttelsesforordningen og den tilhørende Quickguide til GDPR-henvendelser. Dette regelsæt indeholder alle henvendelser i relation til GDPR; med undtagelse af henvendelser om brud på persondatasikkerheden, som er beskrevet i en selvstændig vejledning (jf. afsnit 3.2.5).

Ad g) Databehandleraftalen i medfør af litra g
Aftalens bestemmelse 11 om Sletning og returnering af oplysninger af oplysninger er i overensstemmelse med artikel 28, stk. 3g.

SAM skal enten slette eller alternativt tilbagelevere alle personoplysninger til kunden, efter at behandlingen er ophørt. Det er kunden, der afgør, om SAM skal foretage en sletning eller tilbagelevering af de pågældende oplysninger.

Fortegnelsen over behandlingsaktiviteter indeholder flere it-systemer, der indeholder følsommere personoplysninger. Der gælder for disse systemer at "Personoplysningerne opbevares hos databehandleren, indtil den dataansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret".

Der findes ikke en egentlig skriftlig procedure, men i Finansministeriets slettepolitik henvises der til Finansministeriets myndigheder, der gennem tilsyn følger op på, at databehandlere (SIT og SAM) og deres eventuelle underdatabehandlere, som behandler oplysninger på vegne af myndighederne, sletter personoplysninger i overensstemmelse med databehandleraftalerne.

Ad h) Databehandleraftalen i medfør af litra h
Aftalens bestemmelse 12 om Revision, herunder inspektion er i overensstemmelse med artikel 28, stk. 3h.

Når man som dataansvarlig benytter sig af databehandlere, skal man – udover at indgå en databehandleraftale – kontrollere behandlingen af personoplysninger hos databehandleren. CTJ afgiver en årlig tilsynsrapport vedrørende SAM som databehandler. Denne rapport dokumenterer SAM's overholdelse af indgåede databehandleraftale.

Delresultat
CTJ vurderer, at SAM opfylder sine forpligtelser som databehandler. De indsatte bestemmelser i forordningens § 28 er efter CTJ's opfattelse overholdt.

3.2.3 Krav til indholdet af databehandlerens fortegnelse (artikel 30, stk. 2)

Databehandleraftalen i medfør af artikel 30.2
SAM skal føre en fortegnelse over alle de kategorier af behandlinger, som SAM behandler på vegne af kunden. Fortegnelsen skal leve op til kravene i litra a-d.

Efter litra c skal SAM, hvor det er relevant, medtage oplysninger om overførsler af personoplysninger til et tredjeland.

SAM skal desuden, hvis det er muligt, medtage en generel beskrivelse af de tekniske og organisatoriske foranstaltninger omhandlet i artikel 32, stk. 1.

SAM ajourfører løbende en fortegnelse over alle behandlingsaktiviteter. Rollen som Databehandler, er anført ud for det pågældende system. Fortegnelsen indeholder oplysninger vedrørende Instrukser, Proces (Aktiv), System (Aktiv), Leverandører (Aktiv) og Liste.

SAM har i august 2025 verificeret

- at der er udarbejdet og vedligeholdt en fortegnelse over aktiver, og at denne fortegnelse indeholder ejere/ansvarlige samt de behandlingsaktiviteter, systemerne har for behandling af personoplysninger. Der er ligeledes påset, at der er udarbejdet og vedligeholdt en vejledning i behandlingssikkerhed og sikkerhedsforanstaltninger, der understøtter fortegnelsen.
- at der ikke er nye systemer, der mangler håndtering i GDPR-systemlisten, og alle nuværende systemer i listen er opdateret.

Delresultat
CTJ vurderer, at SAM opfylder fortegnelseskravet. Der er ingen formkrav til fortegnelsen, udover at den skal foreligge skriftligt, herunder elektronisk.

3.2.4 Behandlingssikkerhed – passende sikkerhedsniveau (artikel 32)

Databehandleraftalen i medfør af artikel 32
Aftalens bestemmelse 6 om Behandlingssikkerhed er i overensstemmelse med artikel 32.

Artikel 32 er central og stiller kravene til behandlingssikkerhed. Bestemmelsen i stk. 1 pålægger både kunden og SAM at gennemføre passende foranstaltninger for at sikre et sikkerhedsniveau, der passer til risiciene ved behandlingen. Risikovurderingen skal efter stk. 1 tage hensyn til følgende:

- det aktuelle tekniske niveau,
- implementeringsomkostningerne,
- den pågældende behandlings karakter, omfang, sammenhæng og formål og
- risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

Et passende sikkerhedsniveau vil – i lyset af ovenstående – afhænge af, hvilke og hvor store risici der er for sikkerhedsbrud og dermed for, at fysiske personers rettigheder og frihedsrettigheder krænkes. Overvejelse om behandlingssikkerhed og foranstaltninger skal foretages med regelmæssige mellemrum for at kunne imødegå ændringer i risikobilledet som følge af blandt andet tekniske og organisatoriske foranstaltninger hos kunden eller hos SAM samt ændrede trusler fra omverdenen og internt i organisationen.

SAM udarbejder en risikovurdering i Q4. I risikovurderingen indgår også konsekvens for "brud på registreredes rettigheder og frihedsrettigheder", samt trusler mod den registrerede. Alle aktiver vurderes for sandsynlighed for hændelser, som har indvirkning på den registreredes rettigheder og frihedsrettigheder. Ud fra vurderingen af konsekvens og sandsynlighed for den registreredes rettigheder og frihedsrettigheder udregner SAM den samlede risiko for den registreredes rettigheder og frihedsrettigheder. I den seneste risikovurderingsrapport har SAM ikke registreret processer, it-services eller leverandører med risiko "Middel" (risikoscore over 40).

SAM har i vejledning om Behandlingssikkerhed og sikkerhedsforanstaltninger beskrevet forordningens krav om behandlingssikkerhed ved anvendelse af tekniske og organisatoriske foranstaltninger, samt en konkret beskrivelse af, hvordan SAM sikrer at kravene efterleves. Risikovurderingerne gennemføres, som beskrevet i vejledning for risikovurdering og risikostyring, og dokumenteres i et ISMS-værktøj.

SAM har i september 2025 tilrettet ovennævnte vejledning med beskrivelse af følgende afsnit:

- "Niveauet for behandlingssikkerheden er for hvert system noteret i den nyeste version af "*Oversigt over behandlingsaktiviteter*" i kolonne Q "*Behandlingssikkerhed*". Der skelnes mellem 4 niveauer, som afspejler, hvem der har ansvaret for at tilsikre nødvendige sikkerhedsforanstaltninger. De organisatoriske og tekniske foranstaltninger er beskrevet i samme dokument i fanen '*Instrukser*'. Implementerede sikkerhedsforanstaltninger i de systemer Statens Administration anvender til sin behandling af personoplysninger på vegne af kunderne, er beskrevet i standard databehandleraftalens bilag "*C.2. Behandlingssikkerhed*". Det er med afsæt i efterlevelse af de krav der stilles til statslige myndigheder jf. de 29 tekniske minimumskrav. Foranstaltningerne dækker områderne kryptering, backup, test af effektivitet, adgang via internettet, beskyttelse under transmission, beskyttelse under opbevaring, fysisk sikring, hjemmearbejde og logning".

- "Statens Administration sikrer, i samarbejde med Statens IT, implementering af de nødvendige foranstaltninger. Statens Administration foretager årligt gennemgang af Finansministeriets Center for Tilsyn og Juras tilsynsberetning med Statens IT".

I tabellen gengives de aftalte foranstaltninger, og hvordan de dokumenteres, gennemføres og kontrolleres.

Tabel 4

Passende tekniske og organisatoriske foranstaltninger

Foranstaltning	Dokumentation	Gennemført	Planlagt og udført tilsyn
Pseudonymisering og kryptering af personoplysninger	Teknisk minimumskrav 3, 24 og 27	Opfyldt krav	Tilsyn med kryptografi i SIT
Evnen til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester	Adgang, backup og sikkerhedshændelser i SIT		Tilsyn med adgangsstyring, sikkerhedskopiering og incidenthåndtering i SIT
Evnen til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse	Beredskabsplan og nødplaner i SAM	Udført, dog med et igangværende projekt "Nødplaner"	Tilsyn med beredskab i SAM
Procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden	Test af beredskab og egenkontrol i SAM samt sårbarhedsscanning .	Udført	Tilsyn med test af beredskab, egenkontrol og tilsyn med intern leverandør (SIT) i SAM
Adgang til oplysningerne via internettet	Teknisk minimumskrav 11	Opfyldt krav	Tilsyn med adgangsstyring i SIT
Beskyttelse af oplysninger under transmission	Jf. kryptering	Opfyldt krav	Jf. tilsyn med kryptografi
Beskyttelse af oplysninger under opbevaring	Jf. backup og kryptering	Opfyldt krav	Jf. tilsyn med sikkerhedskopiering og kryptografi
Fysisk sikring af lokaliteter, hvor der behandles oplysninger	Arsenalvej 33, 9800 Hjørring	Udført	Tilsyn med fysisk sikkerhed i SAM
Anvendelse af hjemme-/fjernarbejdspladser	Teknisk minimumskrav 2	Opfyldt krav	
Logning	Teknisk minimumskrav 16	Opfyldt krav	Tilsyn med logning og overvågning i SIT

Anm.: Alle de gennemførte tilsyn med områder i SITs standard drift kan ses i CTJs beretning med SIT
Kilde: SAM – Opfølgningsskema for de tekniske minimumskrav 2025 og CTJ – Tilsynsplan 2025 for gennemgang af SIT Standard drift

Delresultat

CTJ vurderer, at SAM i tilstrækkelig grad har foretaget en risikovurdering. SAM tager hermed stilling til de risici, der er forbundet med behandlingen af personoplysninger,

herunder risikoen for de registrerede. Tilsynet har fået dokumenteret, at risikovurderinger foretages hvert år og godkendes på ledelsesniveau.

Desuden vurderer CTJ, at SAM efterlever de aftalte krav til foranstaltninger i databehandleraftalen. Denne vurdering er underbygget af tilsynet med informationssikkerhedsstyring i SAM og SAM's etablering af tekniske minimumskrav. Heraf er flere krav omfattet af de standardservices, som leveres af SIT. Services er omfattet af CTJ' rotationsplan for tilsyn med SIT.

3.2.5 Anmeldelse og underretning om brud på persondatasikkerheden (artikel 33 stk. 2)

Databehandleraftalen i medfør af artikel 33.2
Aftalens bestemmelse 10 om Underretning om brud på persondatasikkerheden er i overensstemmelse med artikel 33, stk. 2.

Pligten til at anmelde til Datatilsynet påhviler den dataansvarlige, jf. databehandleraftalen. Efter stk. 2 skal SAM uden unødig forsinkelse underrette kunden efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden. SAM skal konstatere, om der er sket et sikkerhedsbrud og herefter underrette kunden samt bistå med informationer til den dataansvarlige for, at denne kan foretage den påkrævede vurdering af, om der skal ske anmeldelse til Datatilsynet og/eller underretning af de registrerede. Det vil sige at SAM ikke kan undlade at underrette kunden om et brud på persondatasikkerheden med henvisning til, at SAM selv har vurderet, at det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder og frihedsrettigheder.

Vejledning i anmeldelse og underretning indeholder blandt andet en beskrivelse af GDPR' krav om

- at *underrette* den dataansvarlige om brud på persondatasikkerheden uden unødig forsinkelse, senest 24 timer efter at være blevet bekendt med bruddet og
- at *bistå* den dataansvarlige i at afdække de nærmere omstændigheder og konsekvenser ved brud på persondatasikkerheden samt
- at kravene *efterleves* af SAM.

På de kvartalsvise informationssikkerhedsudvalgsmøder bliver de fremlagte informationssikkerhedsrapporter gennemgået. Oplysninger om brud på persondatasikkerheden er et fast punkt i rapporten. Blandt andet har SAM ved brud på persondatasikkerheden underrettet kunden uden unødige ophold og om muligt senest 24 timer efter kendskab til bruddet i de fleste tilfælde. I februar og maj var der i alt 5 tilfælde, hvor der ikke skete rettidig underretning. Den seneste rapport samt oplysninger fra SAM viser den seneste udvikling i anmeldte brud. Tallene er gengivet nedenfor.

Kvartal	2022	2023	2024	Pr. 1. december.2025
Q1	18	33	27	18
Q2	21	26	23	19
Q3	23	13	16	32
Q4	23	25	13	12
I alt	**85**	**97**	**79**	**81**

I forbindelse med brud på persondatasikkerheden anvender SAM flere forskellige elementer i processen, såsom

- Opdatering af procedurer for håndtering af brud på persondatasikkerheden.
- Registrering af alle anmeldte brud i oversigt "Brud på persondatasikkerheden".
- Underretning af kunden om et brud uden unødig forsinkelse.
- Læring af tidligere brud på persondatasikkerheden på månedlige møder mellem teamledere i SAM Løn og refusion og SAM Sikkerhed (flest brud i team Løn og refusion).
- Deling af information, der opnås i forbindelse med brud, på de kvartalsvise informationssikkerhedsudvalgsmøder. Eventuel beslutning om awareness, tiltag eller andre initiativer træffes på møderne.

Delresultat
CTJ vurderer, at SAM opfylder underretningspligten. CTJ har løbende fulgt SAM's bestræbelser på at nedbringe de anmeldte brud, og vil fortsat følge initiativerne i tilsynet for 2026.

3.2.6 Konsekvensanalyse vedr. databeskyttelse og forudgående høring (artikel 35, 36 og 28, stk. 3f)

Databehandleraftalen i medfør af artikel 28f
Aftalens bestemmelse 9 om Bistand til den dataansvarlige er i overensstemmelse med artikel 28, stk. 3f.

Pligten til at udarbejde konsekvensanalyse påhviler den dataansvarlige. SAM skal bistå kunden i forbindelse med, at kunden skal sikre overholdelsen af:

- Forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

- Forpligtelsen til at høre Datatilsynet inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af kunden for at begrænse risikoen.

Artikel 36 er nært beslægtet med artikel 35 om udarbejdelse af konsekvensanalyser. Efter artikel 36 skal kunden høre Datatilsynet inden behandling, hvis en konsekvensanalyse vedr. databeskyttelse foretaget iht. artikel 35 viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af kunden for at begrænse risikoen.

Delresultat
SAM har ikke modtaget anmodninger siden henvendelsen fra BM i april 2024.

3.3 Kontrol med SAM som databehandler

Kunden, der som følge af kongelig resolution benytter sig af SAM som databehandler, skal indgå en databehandleraftale med SAM om behandlingen af personoplysninger. I aftalens afsnit 12 om Revision, herunder inspektion, udfører Finansministeriets departement tilsynet med SAM. CTJ udarbejder årligt en tilsynsberetning med SAM, hvor rapporter af gennemførte it-revisioner og tilsynsundersøgelser i indeværende år omtales. Rapporter med forhold i konklusionen omtales i tilsynsberetningen.

Kunden skal forholde sig efterfølgende til de rejste forhold – om et forhold har indvirkning på det område, som kunden som dataansvarlig er ansvarlig for, f.eks. i forbindelse med en risikovurdering eller en regulering i forbindelse med databehandleraftalen.

Tilsynet med SAM som databehandler, er afsluttet uden afgivelse af tilsynsbemærkninger.

Center for Tilsyn og Jura
Finansministeriet, den 15. december 2025

Pia Sønderlund Nielsen
Koncerntilsynschef

Michael Rasmussen

fm.dk