FINANSMINISTERIET

Tilsyn med SAM som databehandler

TR 2/2024 - it-tilsyn - December 2024

Indhold

Tilsynsrapport om tilsyn med SAM som databehandler
TR 2/2024

Denne tilsynsrapport er udarbejdet af:
CTJ/MRA
19-12-2024

Tilsynsrapporten er sendt til:
Att.: Økonomistyrelsen konst. Direktør Signe Caspersen
Statens Administration Direktør Trine Nielsen

1. Konklusion

Center for Tilsyn og Jura (CTJ) i Finansministeriets departement har i november 2024 afsluttet vores tilsyn med Statens Administration (SAM) som databehandler for 2024.

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 ISO27001), 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.	

SAM foretager på vegne af den dataansvarlige (kunden) 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.

Tilsynet har vist, at SAM efterlever de krav, der er fastsat i artikel 28, og som blandet andet fastlægger, at SAM kun må behandle personoplysninger efter instruks fra kunden, herunder hvorvidt SAM kan overføre personoplysninger til et tredjeland eller en international organisation, og at SAM iværksætter passende foranstaltninger.

Tilsynet har også vist, at SAM i forbindelse med brud på persondatasikkerheden anvender flere forskellige elementer i processen, jf. bullets.

- 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.
- Deling af information, der opnås i forbindelse med brud, på de kvartalsvise informationssikkerhedsudvalgsmøder. Evt. beslutning om awareness, tiltag eller andre initiativer træffes på møderne.

Det er CTJ´s indtryk, at SAM gør en del for at reducere antallet af brud. Der ses en stagnation i forhold til tidligere års antal. CTJ vil fortsat følge området.

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's 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 evt. få indtryk af observationer hos SAM.

3. Resultat

3.1 Det overordnede grundlag

Behandling af personoplysninger er aftalt 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's krav til behandling og sikkerhed. Kunden har fortsat ansvaret som dataansvarlig, og dette ansvar overgår således ikke til SAM ved ressortoverførslen.

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

3.2 Etablering af dokumentation

Med baggrund i tilsynets vurderinger foretages der i tabel 2 en bedømmelse ud for de enkelte kontrolmål. I kolonne 3 vurderes det, om SAM kan dokumentere en opfyldelse af krav i GDPR. I kolonne 4 vurderes det, om SAM kan dokumentere en effektiv behandling af personoplysninger i henhold til databehandleraftalen med tilhørende instruks fra kunden.

Tabel 2
Artikler og kontrolmål, som er databehandlerens ansvar

Artikel	Kontrolmål	Opfylde GDPR krav	Effektiv behandling
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.		I/A
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 behandling-		I/A

Tabel 2
Artikler og kontrolmål, som er databehandlerens ansvar

Artikel	Kontrolmål	Opfylde GDPR krav	Effektiv behandling
	en 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.

Nedenfor redegøres der nærmere for tilsynets vurderinger i tabel 2.

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

Iht. 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 standarddatabehandleraftale, som reguleres løbende med ændringer/afvigelser fra Datatilsynets skabelon. I 2024 foreligger der aftaler med alle kunder i SAM. Den seneste version af aftalen er fra juli 2023.

SAM har i august 2024 udført kontrol af "Krav til fortroligheds- og hemmeligholdelsesaftaler, der afspejler organisationens behov for at beskytte information, bør identificeres, gennemgås regelmæssigt og dokumenteres". SAM har verificeret, at der er fortroligheds- og hemmeligholdelsesaftaler i såvel databehandleraftaler med kunder og leverandører.

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 dokumenteret 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 Løn, Regnskab og Refusion (bilag A). Efterlevelse af databehandleraftalens forpligtelser foretages her i tilsynsrapporten.		I/A
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.	I/A	
28,3 c	Iværksætte alle foranstaltninger, som kræves iht. A 32 om behandlingssikkerhed.	Jf. A 32-foranstaltninger.	I/A	
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.		I/A
28,3 f	Bistå kunden med at sikre overholdelse af forpligtelserne efter artikel 32-36.	Jf. A 32-foranstaltninger. Jf. A 33,2-underretning om brud. Jf. A 35/36-konsekvensanalyse og forudgående høring.af DT	I/A	
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.		I/A
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.	Jf. tilsynsrapport og fremlæggelse af resultatet på et kundemøde.	I/A	

Anm.: Vurdering opdeles i en kravsopfyldelse og i en effektivitet. Trafiklys grøn, gul og rød er anvendt.

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 en 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's 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. 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. 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.

SAM's vurdering af resultaterne i CTJ's beretning om tilsynet med Statens It (SIT) og tilsynsrapport om SIT's rolle som databehandler har ikke givet anledning til at udarbejde ISMS afvigelse eller handlingsplan for aktiviteter, som skal udføres i SAM i 2024. Derudover har SAM ikke modtaget underretning om brud på personsikkerhed i 2024. Der foreligger et leverandørtilsynsnotat vedrørende SIT for 2024.

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. 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. Endvidere 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 ift. 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. 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. 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 endvidere, hvis det er muligt, medtage en generel beskrivelse af de tekniske og organisatoriske foranstaltninger omhandlet i artikel 32, stk. 1.

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

SAM har i august 2024 udført kontrol af "Aktiver i relation til information og informationsbehandlingsfaciliteter bør identificeres, og der bør udarbejdes og vedligeholdes en fortegnelse over disse aktiver". Det er verificeret, at der forefindes en fortegnelse over aktiver samt at denne løbende er opdateret og vedligeholdt.

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. 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 fra december 2023 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.

I databehandleraftalens bilag C.2. Behandlingssikkerhed er der blandt andet anført, at databehandleren er berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske foranstaltninger, der skal gennemføres for at etablere det nødvendige (og aftalte) sikkerhedsniveau. Databehandleren skal dog - under alle omstændigheder og som minimum – gennemføre flere foranstaltninger, som er aftalt med den dataansvarlige. De aftalte krav til foranstaltningerne er fremført i bilaget.

En del af de aftalte krav er implementeret af SAM i forbindelse med opfyldelse af de tekniske minimumskrav, og flere krav sker opfyldelsen ved CTJ's tilsyn med informationssikkerheden i Finansministeriets institutioner. SAM foretager herefter en vurdering af relevante forhold i blandt andet CTJ's beretning med SIT i et leverandørnotat. I år har SAM konkluderet, at der ikke er behov for at udarbejde ISMS afvigelse eller handlingsplan for aktiviteter, som skal udføres i SAM i 2024.

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.

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

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

Pligten til at anmelde til Datatilsynet påhviler den dataansvarlige, jf. databehandleraftalerne. 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. Dvs. 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.

SAM har i vejledning om brud på persondatasikkerheden i SAM – anmeldelse og underretning – beskrevet GDPR's krav om anmeldelse af brud på persondatasikkerheden til Datatilsynet og underretning om brud på persondatasikkerheden til den registrerede, samt en konkret beskrivelse af, hvordan SAM sikrer, at kravene efterleves.

Alle brud på persondatasikkerheden registrerer SAM i en oversigt. I september viste oversigten 66 brud i 2024 (75 brud pr. 30.11.2024). Når et brud konstateres – eller har mistanke om – benyttes en proces (jf. vejledning), hvor blandt andet DPO underrettes (og evt. inddrages) og indberettes til kunden uden unødigt ophold og om muligt senest 24 timer efter kendskab til bruddet.

På de kvartalsvise informationssikkerhedsudvalgsmøder bliver de fremlagte informationssikkerhedsrapporter gennemgået. Blandt andet om der er sket en rettidig underretning af den dataansvarlige. Dette er sket i alle tilfælde. I et enkelt tilfælde har behandlingstiden været på over 100 timer, hvor personoplysninger var lækket i SKS ved forkert manuel indtastning. Den sene underretning var sket på baggrund af en menneskelig fejl, hvor SAM's medarbejder ikke fik sendt underretning ved første sagsbehandling. Da SAM blev opmærksom på, at kunden ikke var underrettet, skete der øjeblikkelig underretning.

SAM har skærpet fokus på nedbringelsen af sikkerhedshændelser, men har ikke implementeret tiltag mod sikkerhedshændelser i 2024. Der arbejdes løbende med awareness, f.eks. awareness på kaffemaskine (månedlig), nyhed på intranet, forskelligt mødeforum og kursus. Herudover drøftes sikkerhedshændelser på informationssikkerhedsudvalgsmøderne via gennemgang af den månedlige informationssikkerhedsrapport. Der afholdes desuden månedlige møder mellem teamledere i SAM Løn og refusion og SAM Sikkerhed, med fokus på læring af tidligere brud på persondatasikkerheden.

I den seneste informationssikkerhedsrapport fra september 2024 er der blandt andet anvendt en tabel, som viser udviklingen i anmeldte brud. Tabellens tal er gengivet nedenfor.

Kvartal	2022	2023	pr. 30.11.2024
Q1	18	33	27
Q2	21	26	23
Q3	23	13	16
Q4	23	25	(9)
I alt	85	97	66 (75)

I oversigten over brud har SAM anført, at de fleste brud er sket ved en menneskelig fejl (64 ud af 66). Derfor arbejder SAM løbende med awareness, hvor de gennemførte aktiviteter registreres i en oversigt. I september er der gennemført 19 forskellige awarenesskampagner i 2024.

SAM har også haft særligt fokus på at kortlægge hvilke processer, der er anledning til brud på persondatasikkerheden. Det umiddelbare billede viste, at der skete menneskelige fejl i mange forskellige processer, hvor der behandles personoplysninger på vegne af alle løns og regnskabs kunder. Der er ikke i 2024 identificeret nogle foranstaltninger, der kan reducere antallet af menneskelige fejl i SAM's processer. Teamlederne i løn er opmærksomme på udfordringen og deltager aktivt på de månedlige møder med SAM Sikkerhed.

Delresultat
CTJ vurderer, at SAM opfylder underretningspligten. CTJ vil fortsat følge SAM´s bestræbelser på at nedbringe de anmeldte brud.

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. 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 modtaget én anmodning om bistand til udarbejdelse af konsekvensanalyse fra Beskæftigelsesministeriet angående udvikling af robot til F2.

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. 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 19. december 2024

Pia Sønderlund Nielsen
Koncerntilsynschef

Michael Rasmussen

fm.dk