FINANSMINISTERIET

Tilsynet med SAM som databehandler

August 2022

2021

Konklusion

Kontor for Revision og Tilsyn (KRT) i Finansministeriets departement har afsluttet tilsynet med Statens Administration (SAM) som databehandler for 2021. Tilsynet med SAM omfatter de forpligtelser, der påhviler SAM som databehandler i henhold til databeskyttelsesforordningen (GDPR).

KRT konkluderer overordnet således:

Vurderingsgrundlag	Samlet modenhedsvurdering
Basal beskyttelse, fx kravene til databehandlere og databehandler-aftalen samt indholdet af databehandlerens fortegnelse	Høj beskyttelse
Effektiv beskyttelse, fx procedurer og foranstaltninger samt risiko-vurdering og -styring,	Effektiv beskyttelse

SAM har indgået skriftlige databehandleraftaler med alle kunder om at behandle personoplysninger på deres vegne.

Det gennemførte tilsyn har vist, at SAM efterlever de krav, der er fastsat i databeskyttelsesforordningens artikel 28, og som bl.a. fastlægger, at SAM kun må behandle personoplysninger efter instruks fra kunden (aftalens bilag A og C), herunder hvorvidt SAM kan overføre personoplysninger til et tredjeland eller en international organisation, og at SAM iværksætter passende foranstaltninger.

Det gennemførte tilsyn viste også, at SAM

- ikke har overført personoplysninger til et tredjeland eller en international organisation,
- ikke har modtaget krav om at slette eller tilbagelevere alle personoplysninger til kunden,
- kun har anvendt de godkendte underdatabehandlere i bilag B til databehandleraftalen, herunder en årlig vurdering,
- har vurderet det sikkerhedsmæssige niveau for SAM, herunder de risici, der er forbundet med behandlingen af personoplysninger,
- har underrettet kunden om brud på persondatasikkerheden og
- har udarbejdet dokumentation, som omfatter vejledninger, kontroller (reviews) og andre dokumenter.

KRT fører regelmæssige tilsyn med, at SAM overholder sine forpligtelser, som beskrevet i databehandleraftalen.

KRT's tilsyn har ikke afgivet anledning til bemærkninger.

1. Formål og omfang

KRT 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 de dataansvarliges[1] behov for indsigt i og sikring af SAM's betryggende behandling af personoplysninger som databehandler. KRT'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 den dataansvarliges tilsyn med databehandleren beskrevet og nedenfor gengivet.

"Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af tilsynsmyndigheder".

"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".

"Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivning har adgang til den dataansvarliges og databehandlerens faciliteter, eller repræsentanter, der optræder på myndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation".

Det enkelte tilsyn har til formål at konkludere og rapportere til ledelsen på resultatet af det gennemførte tilsyn.

---

[1] En kunde i SAM er dataansvarlig

2. Resultat

3.1 Det overordnede grundlag

Databehandlerens behandling af personoplysninger sker med henblik på opfyldelse af parternes eksisterende aftalegrundlag "Aftale om levering af administrative service" (kundeaftalen). Kundeaftale samt bilag er indgået på baggrund af den opgaveflytning, der er vedtaget ved kongelige resolution. Den nye databehandleraftale indgås nu som en selvstændig aftale, dvs. ikke som et bilag til kundeaftalen.

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 den dataansvarliges vegne, og hermed skal SAM også opfylde GDPR's krav til behandling og sikkerhed.

KRT's tilsyn med SAM som databehandler udføres med fremsendelse af en spørgeramme i Q2 med deadline for aflevering af svar og materiale i Q3. I Q4 drøftes materialet og der udarbejdes en tilsynsrapport. SAM inddrages løbende i processen og i høringen.

3.2 Etablering af dokumentation

Med baggrund i tilsynets vurderinger foretages en bedømmelse ud for de enkelte kontrolmål. I kolonne 3 vurderes det, om SAM kan dokumentere en overensstemmelse med de relevante 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.

Artikler og kontrolmål, som er databehandlerens ansvar

Artikel	Kontrolmål	Krav i GDPR	Behandle personoplysninger
28 og 29	Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.	Opfyldt	Effektivt
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.	Opfyldt	Effektivt
32	Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske og organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed	Opfyldt	Effektivt
33,2	Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgående databehandleraftale.	Opfyldt	Effektivt
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	Opfyldt	I/A

Artikler og kontrolmål, som er databehandlerens ansvar

Artikel	Kontrolmål	Krav i GDPR	Behandle personoplysninger
	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.	Opfyldt	I/A

Anm.: Bedømt ved grønt trafiklys – opfyldt/effektivt, gult trafiklys – ikke helt opfyldt/effektivt og rødt trafiklys – ikke opfyldt/effektivt.
Kilde: 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 for tilsynets delresultater.

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 har indgået databehandleraftaler med alle kunder. De nye databehandleraftaler, som følger Datatilsynets skabelon, følger lønstandardiseringen og udsendes sammen med de nye kundeaftaler. Pr. 23. august 2021 er der udsendt og underskrevet 53 nye databehandleraftaler i kundeportalen. Ifølge planen har SAM indgået nye databehandleraftaler med samtlige kunder inden maj 2022.

SAM's vurdering af indholdet af Databehandleraftale (kunder) (ISMS kontrolopgave 1450) er udført og godkendt i april kvartal 2021. Det er påset, at der foreligger en standard databehandleraftale til kunder og leverandører. Der er i 2021 udarbejdet ny skabelon for databehandleraftale med kunder.

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 nedenfor og efterfølgende præciseret.

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 den dataansvarliges instruks om behandling af personoplysninger overholdes, foretages i revision/tilsyn af Løn, Regnskab og Refusion (bilag A). Efterlevelse af databehandleraftalens forpligtelser foretages her i tilsynsraporten (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.	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.	
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, fremlæggelse af resultatet på et kundemøde og tilsynsberetning.	I/A

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

Ad a) Databehandleraftalen i medfør af litra a

Aftalens pkt. 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. I databehandleraftalen henvises der til pkt. 8 om overførsel til tredjelande eller internationale organisationer. Hvis overførslen af personoplysninger skal finde sted ifm. brugen af en data-

behandler i et tredjeland, hvor Europa-kommissionen ikke har vurderet, har et tilstrækkeligt beskyttelsesniveau, er der tale om en overførsel til et usikkert tredjeland. I denne situation skal der fremskaffes et overførselsgrundlag, jf. artikel 46 i GDPR.

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 pkt. 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.

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 pkt. 6. Behandlingssikkerhed er i overensstemmelse med artikel 28, stk. 3c.

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

Ad d) Databehandleraftalen i medfør af litra d
Aftalens pkt.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 vejledning af 5. maj 2020 for leverandørstyring beskrevet, hvordan leverandørstyringen håndteres i SAM med fokus på kategorisering af leverandør og revision og tilsyn af leverandører.

SAM's direktør har pr. 27.08.2021 godkendt leverandørtilsynsnotaterne. Notaterne blev forelagt Informationssikkerhedsudvalget til høring den 19.08.2021. Leverandørtilsynsnotaterne for de fem underleverandører er påset af KRT.

SAM har endvidere i vejledning af 23. august 2021 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 pkt. 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 vedr. 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 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 pkt. 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.

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.

SAM har i 2021 ikke modtaget anmodning om sletning eller tilbagelevering af personoplysninger.

Ad h) Databehandleraftalen i medfør af litra h
Aftalens pkt. 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. KRT afgiver nu en årlig tilsynsrapport vedr. SAM som databehandler. Denne rapport dokumenterer SAM's overholdelse af indgåede databehandleraftale.

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

KRT har endvidere vurderet SAM's vurdering af indholdet af Databehandleraftale (ISMS kontrolopgave 1450). Der er ingen bemærkninger hertil.

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.

I SAM ajourføres der 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), Sikkerhedsforanstaltninger, Behandlingsaktiviteter og Liste.

Den seneste oversigt over behandlingsaktiviteter er dateret d. 9. september 2021. SAM's review af fortegnelsen for behandlingsaktiviteter (opgave 1489) er udført og godkendt i juli kvartal 2021. Det er verificeret, at der er beskrevet behandlingsaktiviteter for persondataoplysninger, og at der forefindes en fortegnelse over aktiver (systemer og leverandører), samt at denne løbende er opdateret og vedligeholdt.

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

KRT har endvidere vurderet SAM's review af fortegnelsen for behandlingsaktiviteter (opgave 1489). Der er ingen bemærkninger hertil.

3.2.4 Behandlingssikkerhed – passende sikkerhedsniveau (artikel 32)

Databehandleraftalen i medfør af artikel 32
Aftalens pkt. 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 bl.a. tekniske og organisatoriske foranstaltninger hos kunden eller hos SAM samt ændrede trusler fra omverdenen og internt i organisationen.

SAM har i vejledning om Behandlingssikkerhed og sikkerhedsforanstaltninger beskrevet forordningens krav om behandlingssikkerhed ved anvendelse af tekniske og organisatoriske sikkerhedsforanstaltninger, 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 udarbejdet risikovurdering for 2020. I risikovurderingen indgår også konsekvens for "brud på registreredes rettigheder og frihedsrettigheder", samt trusler mod den registrerede. Alle aktiver er vurderet 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 har SAM udregnet den samlede risiko for den registreredes rettigheder og frihedsrettigheder. For alle aktiver er risiko for den registreredes rettigheder og frihedsrettigheder "Lav" eller "Meget lav" og der iværksættes derfor ikke handlingsplan med udgangspunkt i GDPR.

De implementerede sikkerhedsforanstaltninger pr. system har SAM beskrevet i "GDPR fortegnelse over behandlingsaktiviteter". Flere af de tekniske foranstaltninger er omfattet af KRT's tilsyn med SIT, hvor det centrale it-infrastruktur, herunder netværk, servere og anden it-infrastruktur, som fx understøtter adgangen til administrative systemer jævnfør de fællesstatslige systemer, indgår.

Fra KRT's tilsyn med informationssikkerheden i SAM er de valgte foranstaltninger - der er relevante ift. GDPR - fremført i tabel nedenfor.

Tilsyn og revision af udvalgte og relevante foranstaltninger i 2021

Foranstaltning	ISMS	Vurdering	Bemærkning
Bevidsthed om, uddannelse og træning i informationssikkerhed	7.2.2	Tilfredsstillende	Ingen
Klassifikation af information	8.2.1	Tilfredsstillende	Ingen
Adgangsstyring i NS, SLS og HR-Løn (af Rigsrevisionen)	9.2	Tilfredsstillende	Ingen
Backup af information	12.3.1	Tilfredsstillende	Ingen
Hændelseslogning (SIEM-løsning i SAM)	12.4.1	Tilfredsstillende	Ingen
Håndtering af sikkerhed i Leverandøraftaler	15.1.2	Tilfredsstillende	Ingen
Håndtering af informationssikkerhedsbrud	16.1.5	Tilfredsstillende	Ingen

Supplerende oplysninger:
Ad 7.2.2: SAM afholder løbende awareness-kampagner for forskellige målgrupper i SAM. Oversigten over awareness-aktiviteter viser info om gennemførte aktiviteter, fx om sikkerhedshændelser, Phishing, hjemmearbejde under corona og fysisk sikkerhed i 2021.

Ad 8.2.1: SAM opdaterer efter behov og mindst én gang årligt fortegnelsen over behandlingsaktiviteter. Fortegnelsen omfatter beskrivelse af kritiske aktiver, herunder klassificering.

Ad 12.3.1: SAM har ikke stillet særlige krav om backup af information i kundeaftalen med SIT. SAM benytter SIT´s standardservices inden for området.

Ad 12.4.1: SAM har ikke stillet særlige krav om hændelseslogning i kundeaftalen med SIT. SAM benytter SIT's standardservices inden for området. SAM har 2020 og 2021 År-til-dato ikke haft sikkerhedshændelser, hvor det var nødvendigt at anvende logning fra SIT´s SIEM-system.

Ad 15.1.2: SAM udarbejder årligt tilsynsnotat og evt. handleplan, som bliver forelagt til høring i informationssikkerhedsudvalget og godkendt at SAM´s direktør (formand for informationssikkerhedsudvalget), for hver leverandør. Det udførte tilsyn af SAM foretages efter principperne i tilsynsplanen.

Ad 16.1.5: SAM benytter en proces, hvis man konstaterer – eller har mistanke om – et sikkerhedsbrud. Processen er beskrevet i vejledning om brud på persondatasikkerheden i SAM – anmeldelse og underretning, jf. det efterfølgende afsnit.

Delresultat
KRT 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. 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 pkt. 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 af 9. februar 2020 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 oversigten over sikkerhedshændelser. Pr. 29. juli 2021 har SAM registreret 19 sikkerhedshændelser vedrørende SAM som databehandler. De dataansvarlige er underrettet herom. Hændelserne er lukket.

Delresultat
KRT vurderer, at SAM opfylder underretningspligten.

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

Databehandleraftalen i medfør af artikel 28f
Aftalens pkt. 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 vedr. 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 vedr. 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 i 2021 ikke modtaget anmodning om bistand til udarbejdelse af konsekvensanalyse.

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 FM tilsynet med SAM.

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

Kontor for Revision og Tilsyn
Finansministeriet, den 8. august 2022

Pia Sønderlund Nielsen
Koncerntilsynschef

fm.dk