FINANSMINISTERIET

Tilsyn med SAM som databehandler

TR 2/22 - it-tilsyn - November 2022

2022

Tilsynsrapport vedr. tilsyn med SAM som databehandler

Rapporten er udarbejdet af:
KRT/MRA
10-11-2022

Rapporten er sendt til:
Økonomistyrelsens direktør Maria Schack Vindum
SAM's direktør Trine Nielsen

Indhold

1. Konklusion **4**

2. Formål og omfang **6**

3. Resultat **7**
3.1 Det overordnede grundlag 7
3.2 Etablering af dokumentation 7
3.2.1 Krav til databehandlere (artikel 28, stk. 1) 8
3.2.2 Krav til databehandleraftalen (artikel 28, stk. 3) 8
3.2.4 Behandlingssikkerhed – passende sikkerhedsniveau (artikel 32) 13
3.2.5 Anmeldelse og underretning om brud på persondatasikkerheden (artikel 33 stk. 2) 15
3.2.6 Konsekvensanalyse vedr. databeskyttelse og forudgående høring (artikel 35, 36 og 28, stk. 3f) 17
3.3 Kontrol med SAM som databehandler 18

1. Konklusion

Kontor for Revision og Tilsyn (KRT) i Finansministeriets departement udfører tilsynet med Statens Administration (SAM). Tilsynet med SAM omfatter også de forpligtelser, der påhviler SAM som databehandler i henhold til databeskyttelsesforordningen (GDPR). Kunderne er informeret om tilsynsmodellen i de indgåede databehandleraftaler, og det er heri aftalt, at KRT årligt udarbejder en rapportering om tilsynet med SAM som databehandler, som deles med kunderne.

KRT konkluderer overordnet således:

Tabel 1
Overordnet konklusion

Vurderingsgrundlag	Samlet modenhedsvurdering
Basal 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.	Høj beskyttelse
Effektiv beskyttelse Den effektive beskyttelse sikrer en databeskyttelse gennem: • Internt regelsæt (politikker og procedurer), jf. afsnit 3.2, tabel 3. • Et ledelsessystem (Anneks A i ISO27001), jf. afsnit 3.2.4, tabel 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.	Effektiv beskyttelse

Opgaven, der udføres af SAM som databehandler på vegne af den dataansvarlige (kunden) i SAM, er reguleret i en databehandleraftale. Aftalen beskriver SAM's forpligtelser i relation til behandling af personoplysninger. Disse forpligtelser fremgår af artikel 28 i GDPR.

Det gennemførte tilsyn har vist, at SAM efterlever de krav, der er fastsat i artikel 28, og som bl.a. 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 baseret konklusionen på følgende væsentlige elementer:

- At der foreligger godkendte leverandørtilsynsnotater for de to anvendte underdatabehandlere. De leverancer/services, som SAM modtager fra de pågældende underdatabehandlere, er på et tilfredsstillende niveau.
  På KRT's anbefaling vil SAM fremadrettet anføre i tilsynsnotatet, om SAM for det pågældende år har modtaget underretning ved brud på persondatasikkerheden. SAM har for 2022 oplyst, at de ikke har modtaget underretning om brud ifm. dette års leverandørtilsyn.
- At der foreligger en ajourført oversigt over behandlingsaktiviteter. Endvidere har SAM foretaget et review af oversigten, som ikke gav anledning til yderligere fra SAM.
- At der foreligger en genbesøgt risikovurdering rettet mod de registrerede. SAM har registreret én it-service med risiko "Middel". Handlingsplanens tiltag har SAM afsluttet primo juli 2022.
- At der er iværksat tekniske foranstaltninger efter artikel 32, stk. 1, litra c og d, for at undgå brud på persondatasikkerheden. Flere af foranstaltningerne er omfattet af KRT's tilsyn med SIT. P.t. har vurderingen af det gennemførte tilsyn været tilfredsstillende. En sårbarhedsscanning af diverse sites i SAM har ikke krævet yderligere handling fra SAM.
- At der foreligger en oversigt over sikkerhedshændelser. Oversigten viste en registrering af 38 hændelser i 2022, og 5 hændelser er fortsat i "I gang". KRT har foretaget en vurdering af hændelserne og har haft en dialog med SAM herom. SAM har i 2022 implementeret en række forbedringstiltag, der dels skal mindske antallet af sikkerhedshændelser og dels skal ændre målingen på en underretning til kunden.

KRT's tilsyn har ikke afgivet anledning til bemærkninger.

2. 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.

"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 ledelse og endelig tilsynsrapport for topledelsen i SAM og Økonomistyrelsen.

[1] Kunden i SAM er dataansvarlig. Herefter benævnt som kunde i afsnit 3.

3. Resultat

3.1 Det overordnede grundlag

Behandling af personoplysninger er aftalt i en databehandleraftale mellem en kunde 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.

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 KRT's 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	Behandle personoplysninger
28 og 29	Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede 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 indgåede databehandleraftale.	Opfyldt	Effektivitet
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.	Opfyldt	I/A

Tabel 2
Artikler og kontrolmål, som er databehandlerens ansvar

Artikel	Kontrolmål	Opfylde GDPR krav	Behandle personoplysninger
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

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 har fra februar 2022 anvendt en ny standarddatabehandleraftale ifm. en aftalefornyelse med kunden. Den nye opdaterede databehandleraftale omfatter ændringer foretaget af SAM på 5 bestemmelser (fremgår af aftalens ændringslog).

Med enkelte kunder har SAM indgået databehandleraftaler med særlige krav i bilag C.2 og bilag D, hvor parternes regulering af andre forhold er anført. SAM har foranlediget af KRT's forespørgsel fremsendt den ene aftale, hvori særlige krav til især hjemme-/fjernarbejdspladser, adgang til internettet og logning er aftalt. De særlige krav vil indgå i KRT's samlede vurdering af de implementerede foranstaltninger, der udtages ifm. det regelmæssige tilsyn.

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 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 og fremlæggelse af resultatet på et kundemøde.	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 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 ifm. 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.

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 iht. 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.

I juni 2022 har tilsynsnotaterne for de to godkendte underdatabehandlere i bilag B været en del af høringen i SAM's informationssikkerhedsudvalg. Efterfølgende har SAM's direktør formelt godkendt tilsynsnotaterne. Konklusionen er, at de leverancer/services, som SAM modtager fra de pågældende underdatabehandlere, er på et tilfredsstillende niveau.

SAM's vurdering af de fremhævede forhold i erklæringen har ikke påvirket den service, KMD leverer til SAM, i negativ retning. KRT har gennemset kommenteringen på de enkelte revisionsbemærkninger.

SAM's vurdering af resultaterne i KRT's beretning om tilsynet med SIT har ikke givet anledning til at udarbejde ISMS afvigelse eller handlingsplan for aktiviteter, som skal udføres i SAM i 2022.

SAM har overfor KRT bekræftet, at de ikke i løbet af det seneste år har modtaget underretning ved brud på persondatasikkerheden fra KMD og SIT. Fremover vil denne oplysning fremgå eksplicit af tilsynsnotaterne.

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' 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 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.

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. KRT afgiver en årlig tilsynsrapport vedr. SAM som databehandler. Denne rapport dokumenterer SAM' 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.

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. 4. juli 2022.

Hvert år foretager SAM et review af fortegnelsen for behandlingsaktiviteter. Reviewet for 2022 er udført og godkendt i august 2022. Der er beskrevet behandlingsaktiviteter for persondataoplysninger, og at der forefindes en fortegnelse over aktiver (systemer og leverandører), og at denne er vedligeholdt.

Delresultat
KRT 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 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 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 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 2021 har SAM registreret én it-service med risiko "Middel". Handlingsplanens tiltag har SAM afsluttet primo juli 2022.

De implementerede foranstaltninger 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.

Med baggrund i de planlagte og udførte tilsyn, har KRT udarbejdet en status pr. september 2022 i tabel 4.

Tabel 4
Efterkomme relevante krav alene rent teknisk

Foranstaltning	GDPR	ISO	Udført tilsyn i 2022	Planlagt tilsyn i 2022
Styring af tekniske sårbarheder	Art. 32, stk. 1, litra d	A.12.6.1		Tilsyn med sårbarhedsstyring i SIT
Backup	Art. 32, stk. 1, litra c	A.12.3.1 A.12.2.1	Vurdering af beskyttelse mod malware i SIT var tilfredsstillende.	Tilsyn med sikkerhedskopiering i SIT
Sikring af netværkstjenester	Art. 32, stk. 1, litra d	A.13.1.2		Tilsyn med netværksadministration i SIT
Logning	Art. 32, stk. 1, litra d	A.12.4.1 A.12.4.3		
Undersøgelse af tekniske overensstemmelser	Art. 32, stk. 1, litra d	A.18.2.3 A.12.6.1	Påset sårbarhedsrapporter efter scan af diverse sites i SAM. Der var ingen sårbarheder, der krævede en handling fra SAM.	
Adgangsstyring	Art. 32, stk. 1, litra d	A.9.2		Tilsyn med adgangsstyring i SIT
Fjernarbejdspladser	Art. 32, stk. 1, litra d	A.6.2.2 A.10.1.1 A.15.1.1	Fjernadgang til medarbejdere og leverandører sker gennem VPN (tunnelkryptering) og med 2FA (To-faktor-godkendelse).	
Styring af informationsikkerhedsbrud	Art. 33, stk. 1	A.16.1.1	Jf. afsnit 3.2.5	
Leverandørstyring	Art. 33, stk. 2 Art. 28, stk. 3, litra d	A.15.1.2	Jf. afsnit om litra d i art. 28, stk. 3	

Med baggrund i KRT' beretning med SIT foretager SAM en årlig vurdering af SIT i et tilsynsnotat.

SAM har ingen åbne observationer i 2022 eller i tidligere år med enten høj eller middel risiko.

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. 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 en 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 over sikkerhedshændelser. Oversigten pr. 4. juli 2022 viste, at SAM i 2022 har registreret 38 sikkerhedshændelser, som har kategori "Utilsigtet adgang til data". SAM har noteret, at 5 sikkerhedshændelser er "I gang". 3 af hændelserne er hvor SAM har sendt personoplysninger til den forkerte kunde. Den dataansvarlige (kunden) er underrettet. De 2 andre hændelser er en uhensigtsmæssig proces og et "hul" i ESDH-systemet. En løsning afventer leverandørerne.

På et informationssikkerhedsudvalgsmøde i juni 2022 har SAM haft særlig fokus på det stigende antal sikkerhedshændelser i SAM. Informationssikkerhedsfunktionen i SAM redegjorde for de tiltag, som er foretaget for at mindske antallet af sikkerhedshændelser; herunder awareness samt automatiseringer af materiale til udsendelse. Fx udtræk til kunder og vedhæftninger ifm. regnskabserklæringen.

Informationssikkerhedsfunktionen fremlagde også på informationssikkerhedsudvalgsmødet (ISU) forslag til ændring af KPI'en "Sikkerhedshændelser 01". Hidtil har KPI'en målt på, hvornår en sikkerhedshændelse bliver håndteret af informationssikkerhedsfunktionen i SAM. Det gav mere mening at måle på, om SAM overholder sine forpligtelser over for kunderne jf. databehandleraftalerne – dvs. om SAM får underrettet kunderne/de dataansvarlige indenfor 24 timer, efter SAM er blevet bekendt med bruddet. ISU var enige i ændringsforslaget. Den "nye KPI" anvendes fra og med juni rapporteringen.

I 2022 har SAM bl.a. gennemført awareness om sikkerhedshændelser (præcisering vedr. F2), oplæg om sikkerhedshændelser og cybertruslen på husmøde og oplæg om sikkerhedshændelser på kontormøde i Løn.

Delresultat
KRT vurderer, at SAM opfylder underretningspligten. SAM har i 2022 implementeret en række forbedringstiltag, der dels skal mindske antallet af sikkerhedshændelser og dels skal ændre målingen på en underretning til kunden. Tilsynet vil følge de iværksatte initiativer.

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 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 ikke modtaget anmodning om bistand til udarbejdelse af konsekvensanalyse i 2022.

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. KRT udarbejder årligt en tilsynsberetning med SAM, hvor rapporter af gennemførte it-revisioner og tilsynsundersøgelser i indeværende år omtales. Rapporter med forhold i konklusionen redegøres der for 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, fx ifm. en risikovurdering eller en regulering ifm. databehandleraftalen.

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

Kontor for Revision og Tilsyn
Finansministeriet, den 10. november 2022

Pia Sønderlund Nielsen
Koncerntilsynschef

Michael Rasmussen

fm.dk