Notat

Fra	IT-sikkerhedsgruppen
Sagsnr./Dok.nr.	2023-032351 / 2023-032351-2

03-05-2023

Forvaltningernes bemærkninger til emner i Databeskyttelsesrådgiverens årsrapport 2022

Bilag

Afledte handlinger pr. emne pr. forvaltning:

Sletning

BL	I BL har vi drøftet balancegangen mellem hindring af arbejdsopgaver(forvaltningsloven) sammenholdt med sletningspolitikken, som kan afføde problemstillinger. Denne særskilte betragtning indgår en samlet vurdering fra ”vugge til grav”, hvor alle processer skal indtænkes for at sikre opgaveløsning forekommer ud fra de overordnet retningslinjer. Vi planlægger, at øge korrespondancen og møder med systemansvarlige, således at vi forøger sandsynligheden for alignment på dette processuelle tiltag,
BU	I BU Skal der udarbejdes sletteprocedure for de systemer som har manuel sletning. Derudover bør der laves stikprøvekontrol hvorvidt oplysninger slettes.
JV	I Job og Velfærd anerkender vi, at der bør mere fokus på, at data og oplysninger slettes, når de ikke længere tjener et formål at opbevare. Dog under hensyntagen til, at der ikke sker utilsigtet sletning af relevante personoplysninger, som kan kompromittere tilgængeligheden og integriteten af personoplysninger til skade for borger, samt eventuelle krav ift. arkivering. Forvaltningen har i de senere år sat ekstra fokus på sletning, bl.a. ift. sletningsprocedure ifm. nyanskaffelser, samt udarbejdelse af sletningsinstrukser, som bilag til de allerede indgåede databehandleraftaler. Desuden er ”sletning” i dag blevet en fast del af kravspecifikationen ifm. Nyanskaffelser.
KM	Vi har for nuværende indhentet oplysninger om sletteprocedurer på alle relevante systemer og lagt en plan for, hvilke systemer vi skal starte med at udarbejde sletteprocedurer på.

	Planen beskriver hvordan vi vil arbejde med sletteprocedurer fremadrettet. Vi vurderer, at arbejdet med sletteprocedurer først og fremmest bør prioriteres i forhold til de systemer som er mest "kritiske". Vurderingen af hvilke systemer, der er mest kritiske, bør tage hensyn til karakteren af de personoplysninger, som behandles samt mængden. I denne forbindelse har vi udpeget 4 systemer, som der til en start skal udarbejdes sletteprocedurer på. Der er her tale om en rigtig stor opgave, som vi næppe når i mål med i 2023. Vi bør dog løbende bestræbe os på at få udarbejdet sletteprocedurer på de 4 mest kritiske systemer.
SOM	SOM har gennemgået systemer hvor forvaltningen har systemejerskab og taget stilling til hvilke slettefrister der gælder for data i systemerne. Indstillinger af automatiske sletteregler og arkivering er gennemgået. Fremadrettet har SOM iværksat en opgave med at kontrollere alle systemer for ikke slettede data og der vil i 2023 blive udarbejdet procedurer for kontrol af sletninger – uanset om de sker automatisk eller via en manuel proces Der er en udfordring effektivt at kunne kontrollere om sletning finder sted, da meget af SOMs data ikke må slettes jf. lovgivning for journalføring mm.
SUN	Med ansættelse af en databeskyttelseskonsulent i 2022 og etablering af et GDPR-team, som består af databeskyttelseskonsulenten og IT-sikkerhedslederen, har der igennem 2022 været arbejdet med at systematisere GDPR- og sikkerhedsarbejdet i SUN. Desværre har det ikke været muligt at nå i mål med de opgaver, som blev stillet af DBR. Der arbejdes målrettet på at organisere arbejdet omkring GDPR og IT-sikkerhed på en sådan måde, at opgaverne kan løses indenfor de deadlines, der stilles op. I forbindelse med gentegning af eksisterende kontrakter og ved tegning af nye kontrakter, indgår sletning som et af flere emner, der SKAL indgå i forberedelsesarbejdet forud for indgåelse af en databehandleraftale med en leverandør. I forbindelse med udbud er det en del af kravspecifikationen. Hvis der er tale om et køb, som ligger under udbudsgrænsen, indgår emnerne i dialogen med leverandøren. I fht. de eksisterende aftaler, håndteres emnet ud fra, hvordan det er beskrevet og behandlet i hver af aftalerne.
ØE	Økonomi og Erhverv har arbejdet med sletning på systemniveau, og har generelt fastsat slettefrister efter de anbefalinger der findes i KL's Emnesystematik. Arbejdet med sletning er dog forskelligt fra system til system, da arbejdet afhænger dels af slettefristerne for de pågældende områder og dels systemernes opbygning og tekniske muligheder for at slette. Herudover har Økonomi og Erhverv en række tværgående systemer, hvor arbejdet med sletning skal koordineres med de enkelte forvaltninger og deres afdelinger. Økonomi og Erhverv vil dog i 2. halvår 2023 have fokus på at skabe et samlet overblik over arbejdet med sletning i Økonomi og Erhverv, herunder vurdere om det er muligt at gøre slettefrister mere tydelige i de interne processer.

Kontrol af databehandlere

BL	I BL besidder vi Ca. 35 databehandleraftaler, hvortil der forekommer forskellige kontrolkoncepter. Derudover er vi opmærksom på hvor der kan være anvendt et "forkert" grundlag Fra AAK-skabelon til datatilsynets skabelon kræver tilvænning.
BU	Ingen bemærkninger til denne.
JV	I Job og Velfærd tager vi databeskyttelsesrådgiverens kritik til os. Med udgangspunkt i et meget omfattende IT-systemlandskab, er det en ganske betydelig opgave at føre løbende kontrol med databehandlere. Typisk sker det ved kontrol med revisionserklæringer, der er udarbejdet af uafhængig revisor. Enten erklæringer, der knytter sin til den enkelte IT-leverandør eller det specifikke IT-system (de såkaldte ISAE 3402 erklæringer). Hertil den særlige type af revisionserklæringer, der knytter sig til leverandørens efterlevelse af GDPR (de såkaldte ISAE 3000 erklæringer). I Job og Velfærd har vi ud fra en samlet risikovurdering og prioritering af indsatsen hidtil valgt at gennemføre stikprøver med de modtagne revisionserklæringer og typer. Vi har kun i begrænset omfang gennemført egenkontroller. Udover at være ressourcekrævende kræver det at forholde sig til revisionserklæringer helt særlige kompetencer, som reelt kun to medarbejdere i forvaltningen besidder. Vi ser derfor frem til, at kommunens nylige indtræden i det tværkommunale samarbejde (forening) "Databehandlersekretariatet" forventeligt kan bidrage til et markant løft i den rigtige retning i 2023.
KM	Vi har i 2022 ført tilsyn med systemet GeoEnviron, som er et centralt system i Klima og Miljø. Systemet anvendes til understøttelse af proces for miljøtilsyn, herunder opbevaring af dokumenter og integration til interne systemer. På baggrund af systemets centrale funktion i Klima og Miljø samt mængden af de personoplysninger, der behandles, har vi prioriteret at føre tilsyn med GeoEnviron. Resultatet af vores kontrol samt plan om videre forløb fremgår af vores tilsynsrapport, som er journaliseret i eDoc. Derudover er vi i gang med at udarbejde et styringsdokument, som indeholder et overblik over alle Klima og Miljøs behandlinger. I denne forbindelse vurderer vi for hvert system det enkelte tilsynskoncept, som fremgår af vores databehandleraftaler. Vurderingen af om tilsynskonceptet er tilstrækkeligt foretages på baggrund af Datatilsynets vejledning om tilsynskoncepter. Ud fra et persondataretligt perspektiv er det begrænset hvor mange behandlinger, som vi vurderer, har høj risiko for de registrerede henset til karakteren af de personoplysninger, der behandles. Derfor er forventningen, at vurderingen af hvilket tilsynskoncept, som er tilstrækkeligt vil lempes på mange systemer, så det ikke er nødvendigt at føre tilsyn med visse systemer hvert år. Vi forventer at styringsdokumentet samt vurdering af tilsynskoncepter kommer på plads i 2023.
SOM	SOM har i 2022 forholdt sig løbende til niveauet af nødvendig kontrol for vores databehandlere. Krav til kontrol er et punkt der forhandles i forbindelse med indgåelse af kontrakt og databehandleraftale – men kan også løbende justeres såfremt leverandøren er villig til at indgå i en dialog. Sammenkædning mellem kontrakt, databehandleraftale og kontrolniveau, betyder at kontrolniveauet ikke nødvendigvis kan ændres i en kontrakts løbetid. SOM er derfor meget opmærksom på en grundig kvalitetssikring af nye it-systemer, sådan at arkitekturscreening, risikovurdering og

	DPOens vejledning fremadrettet danner grundlag for krav til leverandørens sikkerhedsniveau, og kontrol af denne.
SUN	GDPR-teamet har systematiseret tilsynet med sine databehandlere og der er generelt en god dialog med leverandørerne, når en databehandleraftale indgås.
ØE	Der arbejdes løbende med udarbejdelse og tilsyn af databehandlere.

Beredskab

BL	- Vi har ca. 20 kritiske systemer, der skal lave beredskabsplaner på. (Alle er indmeldt i ISMS-system) - Beredskabsplan udarbejdes af en GPDR-person samt systemansvarlig. - Vi skal have revurderet hvorvidt alle systemer er kritiske
BU	BU har udarbejdet IT nødplan. BU har i 2023 fokus på at alle afdelinger for nedskrevet procedure ved nedbrud. BU har vurderet at forvaltningen ikke har nogen kritiske systemer. Dog opbevares data vedr. håndtering af medicin både fysisk og digitalt således, at oplysninger altid kan findes.
JV	Job og Velfærd igangsatte et IT-beredskabsprojekt i efteråret 2022, i erkendelse af, at trusselbilledet ift. cyberkriminalitet i dag er langt større og mere reel end tidligere set, i sammenhæng med de afledte konsekvenser af krigen i Ukraine, energikrise og den medfølgende risiko for utilsigtede såvel som planlagte strømsvigt (de såkaldte "brownouts"). Projektet er godt i gang med en allokeret projektleder, der i tæt samarbejde med forvaltningens fagområder, udarbejder planer og foranstaltninger, herunder tests, der kan tage over i en potentiel nødsituation. Ledetråden for projektet er de mest kritiske IT-systemer og aktiver. Høj prioritet har udlevering og håndtering af medicin og forsat mulighed for udbetaling af ydelser. Arbejdet forventes at strække sig over resten af kalenderåret. Job og velfærd deltager også aktivt i det tværkommunale IT-beredskab med fokus på kritisk infrastruktur mv.
KM	I Klima og Miljø er der blevet defineret kritiske IT-funktioner, dem som har kritisk behov for IT-adgang for at kunne fungere – Drikkevandsforsyning, Miljøvagt og Rottebekæmpelse. De har hver især lavet en beredskabsplan for hvordan funktionen varetages uden adgang til IT. Da der skulle laves IT-beredskabsplaner, blev spørgsmålet om kritiske IT- funktioner sendt bredt ud i forvaltningen, og de grupper/teams, der er kommet med tilbagemeldinger, har efterfølgende selv udarbejdet IT-beredskabsplaner. I Teams er IT-beredskabsplanerne tilgængelige for medlemmer i gruppen: AAK – Plan for fortsat drift i krisesituationer. Der er ikke foretaget test af IT-beredskabsplanerne.
SOM	SOM har beredskabsplaner for sine mest kritiske systemer og infrastruktur. Beredskabsplanerne beskriver primært hvordan organisationen skal informeres om nedbrud, hvornår nødprocedurer skal træde i kraft og hvordan eskalering af problemet til leverandører skal håndteres. Langt hovedparten af SOMs systemer er driftet eksternt hos private leverandører. Niveauet af sikkerhed, herunder forhold ved it-nedbrud, hackerangreb, fysiske skader m.m., er reguleret i kontrakt og databehandleraftale på baggrund af en risikovurdering. De primære reguleringsmekanismer i forhold til at en leverandør overholder det aftalte sikkerhedsniveau og opretholder stabil drift er hhv. en Service Level Agreement og en certificering af sikkerhedsniveauet. Service Level Agreement forpligter leverandøren på en bestemt driftstid (typisk over 99% af tiden) og pålægger bod, hvis dette mål ikke nås. Certificeringen (typisk en ISAE 3000) forpligter leverandøren til at etablere bestemte procedurer og beredskaber – f.eks. for backup, genetablering, sikkerhed mod hacking m.v. Certificeringen skal bekræftes årligt af uafhængige IT-revisorer. Evt. justeringer af ovenstående krav til leverandører vil kræve genforhandlinger af kontrakter og databehandleraftaler.

	SOM har på baggrund af en række driftsforstyrrelser i sit mest kritiske IT-system, Cura, påbegyndt dialog med leverandøren omkring en ekstraordinær afprøvning af procedurer for nedbrud og genetablering. Der er endnu ikke truffet nogen endelig aftale. En stor del af SOMs kritiske systemer og processer er afhængige af infrastruktur (strøm, internetforbindelse) og it-integrationer (AD, Fælles Medicin Kort, LOS m.m.) som er ejet og driftet af andre AAK-forvaltninger og myndigheder. Dialog omkring beredskab, driftsstabilitet, overvågning, support og genetablering for denne infrastruktur er et fokusområde for SOM.
SUN	I SUN skal der foretages en kritisk gennemgang af forvaltningens kritiske systemer forud for den kommende risikovurdering. Samtidig får beredskabsplanerne en kritisk gennemgang mhp. eventuel revidering.
ØE	Fra IT-Centret – vedr. kritisk infrastruktur: Backup og restore Vi foretager selv backup af data og systemer på Aalborg Kommunes egne servere. Backuppen opbevares på vores datacenter på Hjulmagervej (den fælles vagtcentral). I 2022 blev indført en ekstra kopi af backuppen (offside backup) som bliver opbevaret hos et eksternt firma. Vi foretager stikprøvevis (én om måneden) restore fra backuppen for at teste at backup-systemerne virker. Populært sagt restorer vi backuppen under et andet navn, så vi ikke forstyrrer den daglige drift. Det er korrekt, at vi ikke lave en egentlig prøvestart af systemet efterfølgende, idet det vil indebære større krav til lukketider, test-servere og involvering af fag-personale. Beredskabsplaner og Disaster/Recovery planer: Der er lavet en beredskabsplan, der overordnet beskriver hvordan vi skal forholde os ved et nedbrud, herunder kommunikation mm. Vi har endvidere lavet diverse dokumenter og planer om reetablering af AD og netværket (det mest basale it-infrastruktur). Disse dokumenter er sikret i et team-site som kan tilgås af nøglepersoner i tilfælde af et større nedbrud. Men det er korrekt at der ikke har været arrangeret en større øvelse i et simuleret totalnedbrud. Der er indgået aftale med eksternt konsulentfirma om at bistå os med at lave en egentlig step by step beskrivelse af hvordan vi kan komme i luften igen efter et større nedbrud, og det vil være naturligt at arrangere en aftestning/øvelse, når denne beskrivelse er færdig. På grund af en overvældende projekt-portefølje har vi desværre måtte skubbe det arbejde foran os, men vi håber at komme i gang med arbejdet efter sommerferien. Nødstrømsanlæg Vi har nødstrømsanlæg i form af dieselgeneratorer på det primære datacenter i Danmarksgade, på det sekundære datacenter på Stigsborg Brygge samt på backup-datacentret på Hjulmagervej. Der er tegnet servicekontrakt med firmaet Coromatic på vedligehold og test af nødstrømanlæg. Dette indebærer bl.a. at generatorerne prøvestartes (og kører tomgang) hvert kvartal. Testrapporter mm. kan findes i eDoc-

	sag 2018-016272. Men det er korrekt, at der ikke foretages en såkaldt knivtest – det vil sige rent faktisk at fjerne bystrømmen til vores datacentre og påse at generatoren starter op, og kan overtage den fulde strømforsyning. Der er planer om at gennemføre en sådan test inden vinteren 2023/2024. I forbindelse med energikrisen i vinteren 2022/2023 fik vi udvidet vores nødstrøm på vore netværksknudepunkter, så alle godt 40 knudepunkter kan holde strøm mindst 2 timer.

Zoom videotjeneste – kommentar fra Job og Velfærd

I Aalborg Kommune anvender vi Teams til videomøder o.l. i de situationer, hvor en ansat i kommunen står som arrangør af møder. Af årsrapporten fremgår, at en enkelt forvaltning imod DBRs anbefaling har valgt at dispensere fra dette og benytter Zoom i relation til en gruppe af borgere.

Her henvises til Job og Velfærd.

Dispensationen er motiveret af, at kunne at tilbyde elektronisk fjernundervisning som supplement til fysisk undervisning, til gavn for borgere tilknyttet Sprogcenter Aalborg.

Dispensationen er specifikt afgrænset til holdundervisning af borgere i tilknytning til sprogcentret, og jævnfør nedenstående begrundet i en samlet risiko- og helhedsvurdering. Herunder vurdering af juridiske, IT-tekniske, såvel som faglige og borgerrelaterede aspekter, der har resulteret i implementering af en række krav og foranstaltninger ifm. brug og anvendelse.

Dispensationen til brug af zoom er initieret af meget dårlige erfaringer med brug af Teams i forhold til denne specifikke form for undervisning. Forvaltningen har ved talrige lejligheder konstateret, at man i forbindelse med brug af Teams til undervisning, ofte bliver smidt af løsningen. Af andre uhensigtsmæssigheder kan nævnes situationer, hvor

- Man kunne ikke dele whiteboard-funktionen (kursisterne kunne ikke se den)
- Flere kursisters chat-funktion virkede ikke (de var logget på teams)
- Indimellem kan man ikke se alle kursister på én gang ligesom i zoom, svært at overskue, hvem der er med.
- En kursist havde kameraet tændt, men underviser kunne ikke se vedkommende.
- Teams arbejder generelt meget langsomt, fx ved oprettelse af private rum i undervisningsøjemed (Modsat Teams har Zoom en ekstra funktionalitet i form af break-out-rooms mv. som understøtter undervisningen)
- Tre kursister blev midt i en undervisningssession smidt af Teams
- En kursist kunne konsekvent ikke komme ind i de private rum og blev smidt af hver gang. Vedkommende mente selv, at hans computer var for gammel - 8 år, men hvis alle ikke kan være med, så fungerer gruppearbejdet og dermed undervisningen ikke.

Vi har ikke afdækket tekniske netværksproblemer i relation til vores kommunale netværk, men i forhold til borgere kan der være sådanne tilfælde, som vi ikke har indflydelse på, dog uden at de synes at optræde i samme omfang ved brug af Zoom. Vi har både i forvaltningen og i samarbejde med IT-centret lavet flere forsøg på at få Teams til at fungere tilfredsstillende til undervisningsbrug i sprogcentret, men hidtil uden held og oplagte alternativer.

Det præciseres, at brug og anvendelse i praksis alene omhandler undervisning og ikke følsomme og fortrolige personoplysninger. Brug af zoom sker ikke ift. sagsbehandling, 1:1 samtaler eller kommunikation og udveksling af fortrolige personoplysninger.