KOMDA

AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. SEPTEMBER 2022 TIL 31. AUGUST 2023 OM BESKRIVELSEN AF HÅNDTERING AF DIGITALE ARKIVALIER OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

BDO

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. SEPTEMBER 2022 TIL 31. AUGUST 2023 OM BESKRIVELSEN AF HÅNDTERING AF DIGITALE ARKIVALIER OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

Til: Ledelsen i KOMDA
KOMDAS kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af KOMDA (databehandleren) for hele perioden fra 1. september 2022 til 31. august 2023 udarbejdede beskrivelse i sektion 3 af håndtering af digitale arkivalier og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelse af personoplysninger i henhold til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) og lov om supplerende bestemmelser til databeskyttelsesforordningen (databeskyttelsesloven), og om udformningen og den operationelle effektivitet af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Databehandlerens ansvar

Databehandleren er ansvarlig for udarbejdelse af udtalelsen i sektion 2 og den medfølgende beskrivelse, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå udtalelsen og beskrivelsen er præsenteret. Databehandleren er endvidere ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, ligesom databehandleren er ansvarlig for at anføre kontrolmålene samt udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

BDO Statsautoriseret revisionsaktieselskab anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om databehandlerens beskrivelse samt om udformningen og den operationelle effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og den operationelle effektivitet af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse samt for kontrollernes udformning og operationelle effektivitet. De valgte handlinger afhænger af databehandlerens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af den operationelle effektivitet af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte kontrolmål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i sektion 2.

Det er vores opfattelse, at det opnåede bevis er tilstrækkeligt og egnet til at danne grundlag for vores konklusion.

Begrænsninger i kontroller hos en databehandler

Databehandlerens beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved anvendelsen af håndtering af digitale arkivalier, som hver enkelt dataansvarlig måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. Herudover er fremskrivningen af enhver vurdering af den operationelle effektivitet af kontroller til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i databehandlerens udtalelse i sektion 2. Det er vores opfattelse:

a. at beskrivelsen af håndtering af digitale arkivalier og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelses af personoplysninger i henhold til databeskyttelsesforordningen og databeskyttelsesloven, således som de var udformet og implementeret i hele perioden fra 1. september 2022 til 31. august 2023, i alle væsentlige henseender er retvisende, og

b. at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. september 2022 til 31. august 2023, og

c. at de testede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som var de, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. september 2022 til 31. august 2023.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, og resultater af disse tests fremgår i sektion 4.

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt dataansvarlige, der har anvendt databehandlerens håndtering af digitale arkivalier, og som har en tilstrækkelig forståelse til at vurdere den sammen med anden information, herunder de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

København, den 15. september 2023

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

Mikkel Jon Larssen
Partner, Chef for Risk Assurance, CISA, CRISC

2. KOMDAS UDTALELSE

KOMDAS varetager behandling af personoplysninger i forbindelse med håndtering af digitale arkivalier for vores kunder, der er dataansvarlige i henhold til Europa-Parlaments og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) og lov om supplerende bestemmelser til databeskyttelsesforordningen (databeskyttelsesloven).

Medfølgende beskrivelse er udarbejdet til brug for de dataansvarlige, der har anvendt håndtering af digitale arkivalier, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

KOMDA anvender underdatabehandler. Denne underdatabehandlers relevante kontrolmål og tilknyttede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller indgår ikke i den medfølgende beskrivelse.

KOMDA bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af håndtering af digitale arkivalier og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller i hele perioden 1. september 2022 til 31. august 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for håndtering af digitale arkivalier og hvordan de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller var udformet og implementeret, herunder redegør for:
    - De typer af ydelser der er leveret, herunder typen af behandlede personoplysninger.
    - De processer i både it-systemer og forretningsgange der er anvendt til at behandle personoplysninger og, om nødvendigt, at korrigere og slette personoplysninger samt at begrænse behandling af personoplysninger.
    - De processer der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige.
    - De processer der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.
    - De processer der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne.
    - De processer der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underretning til de registrerede.
    - De processer der sikrer passende tekniske og organisatoriske sikkerhedsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.
    - De kontroller, som vi med henvisning til afgrænsningen af håndtering af digitale arkivalier har forudsat ville være udformet og implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå kontrolmålene, er identificeret i beskrivelsen.

- De andre aspekter ved kontrolmiljøet, risikovurderingsprocessen, informationssystemerne og kommunikationen, kontrolaktiviteterne og overvågningskontrollerne, som har været relevante for behandlingen af personoplysninger.

2. Indeholder relevante oplysninger om ændringer i håndtering af digitale arkivalier og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der er foretaget i perioden fra 1. september 2022 til 31. august 2023.

3. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af håndtering af digitale arkivalier og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller under hensyntagen til, at denne beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved håndtering af digitale arkivalier, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

KOMDA bekræfter, at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektive i perioden fra 1. september 2022 til 31. august 2023. Kriterierne anvendt for at give denne udtalelse var, at:

1. De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret.

2. De identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål.

3. Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse, i hele perioden fra 1. september 2022 til 31. august 2023.

KOMDA bekræfter, at der er implementeret og opretholdt passende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

Aalborg, den 15. september 2023

KOMDA

Jesper Thomassen
Stadsarkiver

3. KOMDAS BESKRIVELSE AF HÅNDTERING AF DIGITALE ARKIVALIER

KOMDA er en på Aalborg Stadsarkiv funderet afdeling, som indgår aftaler med kommunale §7-arkiver om udførelse af opgaver inden for området digital arkivering. KOMDA tilbyder opbevaring af digitale arkivalier for de deltagende arkiver og giver mulighed for anvendelse af digitale arkivalier gennem udvikling af værktøjer, der tager afsæt i den arkivfaglige kontekst. Derudover står KOMDA for indtag af arkivalier og klargøring af disse til opbevaring, hvilken proces primært udgøres af kvalitetssikring af de modtagne data. Endelig yder KOMDA rådgivningsydelser til de kommuner, der deltager i KOMDA.

Digitale arkivalier er i denne forbindelse data fra offentlige IT-systemer, som er omfattet af bevaringspligt hjemlet i Arkivloven.

KOMDA beskæftiger 3 fuldtidsansatte medarbejdere og trækker på visse ressourcer fra Aalborg Stadsarkiv, herunder IT- og sekretariatsressourcer.

KOMDA'S BEHANDLING AF PERSONOPLYSNINGER

KOMDA fungerer som databehandler for de deltagende, dataansvarlige arkiver og handler udelukkende i henhold til databehandleraftale og efter instruks fra disse. KOMDA leverer i den forbindelse de følgende ydelser, som omfatter behandling af persondata:

- Kvalitetssikring af arkivdata, der modtages fra offentlige myndigheder og afleveres til de deltagende arkiver;
- Opbevaring af arkivdata i flerbenet opbevaringsmiljø, herunder hos underdatabehandler, med hvem der er indgået databehandleraftale;
- Tilgængeliggørelse af arkivdata for de respektive dataansvarlige i tilgængelighedsmiljø på egne servere og via egenudviklet viewer.

De personoplysninger, der behandles, henhører under databeskyttelsesforordningens artikler 6, 9 og 10 og kan således omfatte både almindelige og særlige personoplysninger samt oplysninger om straffedomme og lovovertrædelser.

STYRING AF PERSONDATASIKKERHED

KOMDA har opstillet krav til etablering, implementering, vedligeholdelse og løbende forbedring af et ledelsessystem for persondatasikkerhed, der sikrer opfyldelse af indgåede aftaler med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til Databeskyttelsesforordningen og Databeskyttelsesloven.

De tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller til beskyttelse af personoplysninger er udformet i henhold til risikovurderinger og implementeres for at sikre fortrolighed, integritet og tilgængelighed samt overholdelse af den gældende databeskyttelseslovgivning. Sikkerhedsforanstaltninger og kontroller er efter behov automatiserede og teknisk understøttet af it-systemer.

Styringen af persondatasikkerheden samt de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller er struktureret i følgende hovedområder, for hvilke der er defineret kontrolmål og kontrolaktiviteter:

ARTIKEL	OMRÅDE
Artikel 28, stk. 1	Databehandlerens garantier
Artikel 28, stk. 3	Databehandleraftale
Artikel 28, stk. 3, litra a og h, og stk. 10 Artikel 29 Artikel 32, stk. 4	Instruks for behandling af personoplysninger

ARTIKEL	OMRÅDE
Artikel 28, stk. 2 og 4	Underdatabehandlere
Artikel 28. stk. 3, litra b	Fortrolighed og lovbestemt tavshedspligt
Artikel 28, stk. 3, litra c	Tekniske og organisatoriske sikkerhedsforanstaltninger
Artikel 28, stk. 3, litra g	Sletning og tilbagelevering af personoplysninger
Artikel 28, stk. 3, litra e, f og h	Bistand til den dataansvarlige
Artikel 30, stk. 2, 3 og 4	Fortegnelse over kategorier af behandlingsaktiviteter
Artikel 33, stk. 2	Underretning om brud på persondatasikkerheden.

RISIKOVURDERING

KOMDA's ledelse sørger for, at der iværksættes alle de initiativer, der imødegår det trusselsbillede, som KOMDA står over for, således at indførte sikkerhedsforanstaltninger og kontroller er passende, og risikoen for brud på persondatasikkerheden reduceres til et passende niveau.

Der foretages en løbende vurdering af, hvilket sikkerhedsniveau der er passende. I vurderingen tages der hensyn til risici i forhold til personoplysningers hændelige eller ulovlige tilintetgørelse, tab eller ændring, eller uautoriseret videregivelse af eller adgang til personoplysninger, der behandles af KOMDA. Der er særligt fokus på sidstnævnte, oplysningernes fortrolighed, da et fortrolighedstab vurderes at have de mest graverende konsekvenser for rigtige menneskers rettigheder og frihedsrettigheder.

Som grundlag for ajourføring af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller udføres der en gang årligt en risikovurdering. Risikovurderingen belyser sandsynligheden for og konsekvenserne af hændelser, der kan true persondatasikkerheden og dermed fysiske personers rettigheder og frihedsrettigheder. Risikovurderingen tager hensyn til det aktuelle tekniske niveau og implementeringsomkostningerne.

TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER

De tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller vedrører alle processer og systemer, som behandler personoplysninger på vegne af den dataansvarlige. De i kontrolskemaet anførte kontrolmål og kontrolaktiviteter er en integreret del af den efterfølgende beskrivelse.

DATABEHANDLERENS GARANTIER

KOMDA har indført politikker og procedurer, der sikrer, at KOMDA kan stille tilstrækkelige garantier til at gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder. KOMDA har etableret en organisering af persondatasikkerheden samt udarbejdet og implementeret en af ledelsen godkendt databeskyttelsespolitik, der løbende gennemgås og opdateres. Der forefindes procedurer for rekruttering og fratrædelse af medarbejdere samt retningslinjer for medarbejdere, der behandler personoplysninger og fastholdelse af sikkerhedsbevidsthed hos disse, eksempelvis gennemførelse af awareness- og oplysningskampagner.

DATABEHANDLERAFTALE

KOMDA har indført procedurer for indgåelse af databehandleraftaler, der sikrer, at KOMDA i tilknytning til driftsaftaler med de dataansvarlige indgår en databehandleraftale, der angiver betingelserne for behandling af personoplysninger på vegne af den dataansvarlige. KOMDA anvender en skabelon eller lignende for databehandleraftaler i overensstemmelse med de tjenester, der leveres, herunder information om brugen af underdatabehandlere. Databehandleraftalerne er digitalt underskrevet og opbevares elektronisk.

INSTRUKS FOR BEHANDLING AF PERSONOPLYSNINGER

KOMDA har indført procedurer, der sikrer, at KOMDA handler efter den instruks, som den dataansvarlige har givet i databehandleraftalen. Instruksen opretholdes ved procedurer, der instruerer medarbejderne i, hvorledes behandling af personoplysninger skal ske. Proceduren sikrer desuden, at KOMDA informerer den dataansvarlige, når KOMDA får mistanke om, at den dataansvarliges instruks er i strid med databeskyttelseslovgivningen.

UNDERDATABEHANDLERE

KOMDA indgår aftaler med underdatabehandlere, der sikrer, at underdatabehandlere er blevet pålagt de samme databeskyttelsesforpligtelser, som er anført i databehandleraftalen mellem den dataansvarlige og KOMDA, og at underdatabehandlerne kan give tilstrækkelige garantier til beskyttelse af personoplysninger. Underdatabehandlere anvendes udelukkende til bitbevaring og behandler kun krypterede datapakker, således at underdatabehandleres håndtering af læsbare data elimineres som et risikomoment.

Databehandleraftaler med de dataansvarlige sikrer, at den dataansvarlige giver en forudgående specifik eller generel skriftlig godkendelse af underdatabehandlere, herunder at der sker en styring af ændringer i godkendte underdatabehandlere.

Før indgåelse af nye aftaler med underdatabehandlere, vurderer KOMDA, om disse vil kunne overholde de forpligtelser, som er pålagt KOMDA. KOMDA skal føre et årligt tilsyn med sine underdatabehandlere, baseret på en risikovurdering af den konkrete behandling af personoplysninger.

FORTROLIGHED OG LOVBESTEMT TAVSHEDSPLIGT

KOMDA har indført procedurer, der sikrer fortrolighed ved behandlingen af personoplysninger. Alle medarbejdere i KOMDA har forpligtet sig til tavshed og fortrolighed ved deres ansættelse i Aalborg Kommune og ved at underskrive KOMDA's databehandlerforståelseserklæring.

TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER

Risikovurdering
KOMDA har gennemført de tekniske og organisatoriske sikkerhedsforanstaltninger på baggrund af en vurdering af risici i forhold til fortrolighed, integritet og tilgængelighed. Der henvises til særskilt afsnit herom.

Beredskabsplaner
KOMDA har etableret beredskabsplaner, således at KOMDA indenfor rimelig tid kan genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af fysiske eller tekniske hændelser. Beredskabsplaner sikrer også, at KOMDA kan reagere hurtigt og lovmedholdeligt i tilfælde af en sikkerhedshændelse, der truer personoplysningers fortrolighed.

KOMDA har etableret et kriseberedskab, der træder i kraft i disse tilfælde. Organisering af kriseberedskabsgruppe er etableret, og der indført retningslinjer for aktivering af kriseberedskabet.

KOMDA's beredskabsplaner sikrer personuafhængighed i forbindelse med aktivering af beredskabet og retableringen. Planerne er i kopi opbevaret sikret uden for KOMDA's IT-miljø. Planerne afprøves og revideres løbende i forbindelse med ændringer i systemer mv.

Opbevaring af personoplysninger
KOMDA sørger for, at opbevaring af personoplysninger alene foretages i overensstemmelse med kontrakten med den dataansvarlige og listen over lokationer i den tilhørende databehandleraftale.

Fysisk adgangskontrol
KOMDA har indført procedurer, der sikrer, at lokaler er beskyttet mod uautoriseret adgang. Kun personer med et arbejdsbetinget eller andet legitimt behov har adgang til lokalerne, og særlige sikkerhedsmæssige

foranstaltninger er indført for områder, hvor der foretages behandling af personoplysninger. Kunder, leverandører og andre besøgende ledsages, hvis de skal have adgang til disse områder. Desuden er adgang til persondata altid beskyttet med adgangskoder (til systemer) og kryptering (på medier), således at uvedkommende ikke kan tilgå oplysningerne, selvom de måtte befinde sig i KOMDA's lokaler.

KOMDA har indført procedurer, der sikrer, at adgang til serverrum er tildelt ud fra et arbejdsbetinget behov. Serviceleverandører, der måtte have behov for adgang, godkendes af ledelsen ad hoc og overvåges, mens de er til stede.

Fysisk sikkerhed
KOMDA har indført procedurer, der sikrer, at servere er beskyttet mod uautoriseret adgang, beskadigelse, driftsafbrydelser og lignende hændelser ved særlige sikkerhedsforanstaltninger. Servere er således opbevaret i et særligt indrettet serverrum med fysisk adgangskontrol. Data er sikret mod miljømæssige trusler som brand, vandindtrængning, fugt, overophedning, strømudfald, solstorme og overspænding gennem et system med distribueret opbevaring med flerfoldig redundans, således at beskadigede data vil kunne genetableres fra en af de andre lokationer.

Logisk adgangssikkerhed
KOMDA har indført procedurer, der sikrer, at adgang til systemer og data er beskyttet af et autorisationssystem. Brugere oprettes med unik brugeridentifikation og password, og brugeridentifikation anvendes ved tildeling af adgang til ressourcer og systemer. Al tildeling af rettigheder i systemer sker ud fra et arbejdsbetinget behov der er formuleret i autorisationer for de personer, der skal have adgang til ressourcer og data. Der foretages mindst én gang årligt en evaluering af brugernes fortsatte arbejdsbetingede behov for adgang. Procedurer og kontroller understøtter processer for oprettelse, ændring og nedlæggelse af brugere og tildeling af rettigheder samt gennemgang heraf.

Krav til blandt andet længde, kompleksitet og løbende udskiftning af password samt lukning af brugerkonto efter forgæves adgangsforsøg er restriktive. Der er udformet tekniske foranstaltninger, der understøtter disse krav.

Fjernarbejdspladser og fjernadgang til systemer og data
KOMDA har indført procedurer, der sikrer, at adgang fra arbejdspladser uden for KOMDA's lokaler og fjernadgang til systemer og data sker via krypterede forbindelser med to-faktor autentifikation. Procedurerne omfatter også hensigtsmæssig indretning af hjemmearbejdspladser, herunder acceptabel anvendelse og administration af arbejds-pc'er, anvendelse af skærmlås, beskyttelse mod indkig, skuldersurfing og lignende.

Eksterne kommunikationsforbindelser
KOMDA har indført procedurer, der sikrer, at eksterne kommunikationsforbindelser er sikret med stærk kryptering.

Kryptering af personoplysninger
KOMDA har indført procedurer, der sikrer, at persondata altid er krypteret både i hvile og i transmission. Oplysninger kan være krypterede på fil-, medie- eller filsystemsniveau. KOMDA vedligeholder retningslinjer for, i hvilke sammenhænge de forskellige krypteringsmetoder skal anvendes. Transmission af persondata sker altid over krypterede forbindelser. Genoprettelsesnøgler og opbevares på forsvarlig vis.

KOMDA har indført procedurer, der sikrer, at der ikke behandles persondata på personlige enheder, der ikke er beskyttet af særlige sikkerhedsforanstaltninger, herunder kryptering af hele filsystemet, således at adgang til data alene er mulig for autoriserede brugere, og at slettede persondata ikke vil kunne genskabes.

De algoritmer og niveauer for kryptering, der er anvendt til kryptering af enheder, servere og data, risikovurderes løbende i forhold til det aktuelle trusselsniveau. De valgte krypteringsmetoder fremgår af procedurer.

Firewall
KOMDA har indført procedurer, der sikrer, at trafik mellem internettet og KOMDA's netværk kontrolleres af firewall. Adgang udefra via porte i firewallen er begrænset mest muligt, og adgangsrettigheder tildeles via konkrete porte til specifikke segmenter. Arbejdsstationer benytter firewall.

Netværkssikkerhed
KOMDA har indført procedurer, der sikrer, at netværk i forhold til anvendelse og sikkerhed er opdelt i et antal virtuelle netværk (VLAN), hvor trafik mellem de enkelte virtuelle netværk kontrolleres af firewall. Servere med indbygget firewall benytter denne til at sikre, at der kun gives adgang til nødvendige services.

Antivirusprogram
KOMDA har indført procedurer, der sikrer, at enheder med adgang til netværk og applikationer er beskyttet mod virus og malware. Der sker en løbende opdatering og tilpasning af antivirusprogrammer og andre beskyttelses-systemer i forhold til det aktuelle trusselsniveau, og der er indført procedurer, der sikrer, at antimalware-programmer holdes opdaterede.

Sårbarhedsscanning
KOMDA iværksætter efter behov sårbarhedsscanninger eller penetrationstest. Behov for disse foranstaltninger kan være, at der er blevet ændret i KOMDA's systemlandskab, eller at det er flere år siden, at der sidst er blevet udført slige tests.

Sikkerhedskopiering og retablering af data
KOMDA har indført procedurer, der sikrer, at data i KOMDA's opbevaringsmiljø opbevares redundant på flere forskellige lokationer og forskellige medier for at imødegå tab af data eller tab af tilgængelighed ved nedbrud. Data på forskellige lokationer og medier er beskyttet med fysiske og logiske sikkerhedsforanstaltninger, der forhindrer, at data kommer uvedkommende i hænde.

Vedligeholdelse af systemsoftware
KOMDA har indført procedurer, der sikrer, at systemsoftware opdateres løbende efter leverandørernes forskrifter og anbefalinger. Procedurer for Patch Management omfatter operativsystemer, kritiske services og software installeret på servere og arbejdsstationer.

Logning i systemer, databaser og netværk
KOMDA har indført procedurer, der sikrer, at logning er opsat i henhold til forretningsmæssige behov, baseret på en risikovurdering af systemer og det aktuelle trusselsniveau. Omfang og kvalitet af log-data er tilstrækkelig til at identificere og påvise eventuelt misbrug af systemer eller data, og logdata gennemgås løbende for anvendelighed og unormal adfærd.

Overvågning
KOMDA har indført procedurer, der sikrer, at der sker løbende overvågning af systemer og indførte tekniske sikkerhedsforanstaltninger.

Reparation og service samt bortskaffelse af it-udstyr
KOMDA har indført procedurer, der sikrer, at udstyr, som udleveres til tredjemand for service, reparation eller bortskaffelse, udleveres uden datadiske, og at brugte og kasserede datamedier og diske og destrueres af en pålidelig leverandør.

Afprøvning, vurdering og evaluering
KOMDA har indført kontroller, der overvåger, at de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden, virker.

SLETNING OG TILBAGELEVERING AF PERSONOPLYSNINGER

KOMDA sletter personoplysninger eller tilbageleverer disse til den dataansvarlige i henhold til instruks og driftsaftale, når behandlingen af personoplysninger ophører ved udløb af kontrakten med den dataansvarlige.

BISTAND TIL DEN DATAANSVARLIGE

KOMDA arbejder efter instruks fra den dataansvarlige. Det betyder, at KOMDA efter instruks yder bistand til den dataansvarlige, når denne skal opfylde sin forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder. Denne bistand kan omfatte søgninger i data, udlevering af søgeresultater, udlevering af arkiveringsversioner, så den dataansvarlige kan foretage sletning osv. KOMDA er i denne forbindelse blot et umælende redskab i den dataansvarliges hånd.

Det samme gør sig gældende i forbindelse med KOMDA's bistand til den dataansvarlige med at sikre overholdelse af forpligtelserne i artikel 32 om behandlingssikkerhed, artikel 33 om anmeldelse og underretning af brud på persondatasikkerheden samt artikel 34 – 36 om konsekvensanalyser. For bistand iht. artikel 33 er der udarbejdet særskilte procedurer.

DEN DATAANSVARLIGES TILSYN MED KOMDA

KOMDA stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene til databehandlere, til rådighed for den dataansvarlige. KOMDA giver desuden mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller andre, som er bemyndiget hertil af den dataansvarlige.

FORTEGNELSE OVER KATEGORIER AF BEHANDLINGSAKTIVITETER

KOMDA fører en fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige. Fortegnelsen opdateres regelmæssigt og kontrolleres under den årlige gennemgang af politikker og procedurer mv. Fortegnelsen opbevares elektronisk og kan stilles til rådighed for tilsynsmyndigheden efter anmodning.

UNDERRETNING OM BRUD PÅ PERSONDATASIKKERHEDEN

KOMDA har indført politikker og procedurer, der sikrer, at brud på persondatasikkerheden registreres med detaljeret information om hændelsen, og at der sker underretning af den dataansvarlige uden unødig forsinkelse, efter at KOMDA er blevet opmærksom på, at der er sket brud på persondatasikkerheden. De registrerede informationer gør den dataansvarlige i stand til at foretage en vurdering af, om bruddet på persondatasikkerheden skal anmeldes til tilsynsmyndigheden, og om de registrerede skal underrettes.

ÆNDRINGER I PERIODEN FRA 1. SEPTEMBER 2022 TIL 31. AUGUST 2023

KOMDA har ikke foretaget væsentlige ændringer i håndtering af digitale arkivalier og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller i perioden fra 1. september 2022 til 31. august 2023.

KOMPLEMENTERENDE KONTROLLER HOS DE DATAANSVARLIGE

Den dataansvarlige er forpligtet til at implementere følgende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller for at opnå kontrolmålene og dermed opfylde databeskyttelseslovgivningen:

1. Den dataansvarlige skal sikre, at instruksen fra den dataansvarlige er lovlig i forhold til den til enhver tid gældende databeskyttelseslovgivning, og at instruksen er hensigtsmæssig i forhold til den indgåede kontrakt og databehandleraftalen.

2. Den dataansvarlige har ansvaret for at sikre, at administratorernes brug af ASDA og den behandling af personoplysninger, der foretages i systemet, sker i overensstemmelse med relevant lovgivning.

3. Den dataansvarlige bestemmer, hvem der skal tildeles adgang til ASDA, og hvilke behandlinger af persondata disse personer må foretage.

4. Den dataansvarlige skal pleje fornuftig omgang med passwords og udstyr, der anvendes til at tilgå den dataansvarliges data i ASDA herunder med enheder, der bruges til at modtage midlertidige passwords som en del af to-faktor-identifikation.

5. Den dataansvarlige skal underrette KOMDA om enhver mistanke om uautoriseret adgang til data i ASDA.

4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST

Formål og omfang

BDO har udført sit arbejde i overensstemmelse med ISAE 3000 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger.

BDO har udført handlinger for at opnå bevis for oplysningerne i KOMDAS beskrivelse af håndtering af digitale arkivalier samt for udformningen og den operationelle effektivitet af de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. De valgte handlinger afhænger af BDO's vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt.

BDO's test af udformningen og den operationelle effektivitet af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af KOMDA, og som fremgår af efterfølgende kontrolskema.

I kontrolskemaet har BDO beskrevet de udførte test, der blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og at de tilhørende kontroller var hensigtsmæssigt udformet og har fungeret effektivt i hele perioden fra 1. september 2022 til 31. august 2023.

Udførte testhandlinger

Test af udformningen af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller samt implementeringen heraf er udført ved forespørgsel, inspektion, observation og genudførelse.

Type	Beskrivelse
Forespørgsel	Forespørgsler hos passende personale er udført for alle væsentlige kontrolaktiviteter. Forespørgslerne blev udført for blandt andet at opnå viden og yderligere oplysninger om indførte politikker og procedurer, herunder hvordan kontrolaktiviteterne udføres, samt at få bekræftet beviser for politikker, procedurer og kontroller.
Inspektion	Dokumenter og rapporter, der indeholder angivelse om udførelse af kontrollen, er gennemlæste med det formål at vurdere udformningen og overvågningen af de specifikke kontroller, herunder om kontrollerne er udformede, således at de kan forventes at blive effektive, hvis de implementeres, og om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Test af væsentlige systemopsætninger af tekniske platforme, databaser og netværksudstyr er udført for at påse, om kontroller er implementerede, herunder eksempelvis vurdering af logning, sikkerhedskopiering, patch management, autorisationer og adgangskontroller, datatransmission samt besigtigelse af udstyr og lokaliteter.
Observation	Anvendelsen og eksistensen af specifikke kontroller er observeret, herunder test for at påse, at kontrollen er implementeret.
Genudførelse	Kontroller er genudført for at verificere, at kontrollen fungerer som forudsat.

For de ydelser, som Det Kongelige Bibliotek leverer inden for opbevaring af digitale arkivalier, har vi modtaget ledelseserklæring omkring informationssikkerhed af 21. september 2022 samt rapport fra databehandlerens kontrolbesøg fra den 25. november 2022, for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

Denne underdatabehandlers relevante kontrolmål og tilknyttede kontroller indgår ikke i KOMDAs beskrivelse af håndtering af digitale arkivalier og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos KOMDA, der sikrer udførelsen af et behørigt tilsyn med underdatabehandlerens opfyldelse af

den mellem underdatabehandleren og databehandleren indgåede databehandleraftale og opfyldelse af databeskyttelsesforordningen og databeskyttelsesloven.

Resultat af test

Resultatet af de udførte test af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller angiver, om den beskrevne test har givet anledning til at konstatere afvigelser.

En afvigelse foreligger, når:

- Tekniske eller organisatoriske sikkerhedsforanstaltninger eller øvrige kontroller mangler at blive udformet og implementeret for at kunne opfylde et kontrolmål.
- Tekniske eller organisatoriske sikkerhedsforanstaltninger eller øvrige kontroller, der knytter sig til et kontrolmål, ikke er hensigtsmæssigt udformet og implementeret eller ikke har fungeret effektivt i perioden.

Artikel 28, stk. 1: Databehandlerens garantier		
Kontrolmål ▶ *At sikre, at databehandleren kan stille de fornødne garantier til beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og beskyttelsen af den registreredes rettigheder.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Informationssikkerhedspolitik ▶ Databehandleren har udarbejdet og implementeret en informationssikkerheds- og databeskyttelsespolitik.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens informationssikkerheds- og databeskyttelsespolitik.	Ingen afvigelser konstateret.
Gennemgang af informationssikkerhedspolitik ▶ Databehandlerens informationssikkerheds- og databeskyttelsespolitik bliver gennemgået, opdateret og godkendt af ledelsen minimum en gang årligt	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens informationssikkerheds- og databeskyttelsespolitikken og observeret, at denne er godkendt af ledelsen i december 2022.	Ingen afvigelser konstateret.
Organisering af informationssikkerhedspolitik ▶ Databehandler har dokumenteret og etableret ledelsesstyrring af informationssikkerhed og databeskyttelsespolitikken.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens gennemgang af informationssikkerheds- og databeskyttelsespolitik og observeret, at ledelsen har gennemgået denne med medarbejderne.	Ingen afvigelser konstateret.
Rekruttering af medarbejdere ▶ Databehandleren udfører screening af potentielle medarbejdere før ansættelse.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for styring af medarbejdere og observeret, at der skal indhentes relevante referencer.	Ingen afvigelser konstateret.

Artikel 28, stk. 1: Databehandlerens garantier		
Kontrolmål ▶ *At sikre, at databehandleren kan stille de fornødne garantier til beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og beskyttelsen af den registreredes rettigheder.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi er på forespørgsel blevet oplyst, at der ikke har været nyansættelser i erklæringsperioden, hvorfor vi ikke har kunnet efterprøve kontrollen.	
Fratrædelse af medarbejdere ▶ Databehandleren har udarbejdet og implementeret en procedure for fratrædelse af medarbejdere ved ophør af ansættelse. ▶ Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for styring af medarbejdere og observeret, at der er en procedure for fratrædelse af medarbejdere. Vi har observeret, at proceduren indeholder retningslinjer for, at medarbejdere ved fratrædelse orienteres om, at fortrolighed forsat er gældende. Vi er ved forespørgsel blevet oplyst, at der har været en fratrædelse i erklæringsperioden. Vi har inspiceret, at der for fratrådt medarbejder i erklæringsperioden, er udfyldt fratrædelsesskema, hvor medarbejder orienteres om fortsat gældende fortrolighedsaftale.	Ingen afvigelser konstateret.
Uddannelse og instruktion af medarbejdere, der behandler personoplysninger ▶ Databehandleren afholder awareness-træning af nye medarbejdere i henhold til databeskyttelse og informationssikkerhed, i forlængelse af ansættelsen. ▶ Der afholdes introduktionskursus for nye medarbejdere, herunder om behandling af dataansvarliges personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for styring af medarbejdere og observeret, at der er angivet, at nye medarbejdere skal introduceres til informationssikkerheds- og databeskyttelsespolitikker samt kurser omkring persondata.	Ingen afvigelser konstateret.

Artikel 28, stk. 1: Databehandlerens garantier		
Kontrolmål ▶ *At sikre, at databehandleren kan stille de fornødne garantier til beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og beskyttelsen af den registreredes rettigheder.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi er på forespørgsel oplyst, at der ikke har været ansættelser i perioden, hvorfor vi ikke har kunnet efterprøve kontrollen.	
Awareness og oplysningskampagner for medarbejdere ▶ Databehandleren fastholder medarbejderes bevidsthed om databeskyttelse og informationssikkerhed.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for styring af medarbejdere og observeret, at medarbejdere skal gennemgå kampagner vedrørende informationssikkerhed og databeskyttelse. Vi har foretaget inspektion af, at alle medarbejdere har gennemgået awareness- og oplysningskampagner.	Ingen afvigelser konstateret.

Artikel 28, stk. 3: Databehandleraftale

Kontrolmål

- *At sikre, at databehandleren indgår en skriftlig kontrakt med den dataansvarlige, der fastsætter vilkårene for behandlingen af den dataansvarliges personoplysninger, og at kontrakten opbevares elektronisk.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Indgåelse af databehandleraftale med den dataansvarlige - Databehandleren har procedurer for indgåelse af skriftlige databehandleraftaler, der er i overensstemmelse med de ydelser, som databehandleren leverer. - Databehandleren anvender en databehandleraftaleskabelon for indgåelse af databehandleraftaler. - Databehandleraftaler underskrives og opbevares elektronisk. - Databehandleraftaler indeholder informationer om brugen af underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for aftaler og observeret, at indgåede databehandleraftaler er i overensstemmelse med de ydelser, som databehandleren leverer. Vi har foretaget inspektion af databehandlerens procedure for aftaler og observeret, at der anvendes en skabelon for indgåelse af aftaler. Vi har observeret, at databehandleraftalerne underskrives og opbevares elektronisk. Vi har foretaget inspektion af skabelon for databehandleraftaler og observeret, at denne indeholder oplysninger om brugen af underdatabehandlere. Vi har stikprøvevis inspiceret indgået databehandleraftale og observeret, at denne indeholder oplysninger om brugen af underdatabehandlere.	Ingen afvigelser konstateret.

Artikel 28, stk. 3 og 10, artikel 29 og artikel 32, stk. 4: Instruks for behandling af personoplysninger		
Kontrolmål ▶ *At sikre, at databehandleren alene handler efter dokumenteret instruks fra den dataansvarlige.* ▶ *At sikre, at databehandleren underretter den dataansvarlige, hvis en instruks er i strid med databeskyttelsesforordningen og databeskyttelsesloven.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Instruks for behandling af personoplysninger ▶ Indgået databehandleraftale indeholder en instruks fra den dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af skabelon for databehandleraftale og observeret, at denne indeholder instruks fra den dataansvarlige. Vi har stikprøvevis inspiceret indgået databehandleraftale og observeret, at denne indeholder instruks fra den dataansvarlige.	Ingen afvigelser konstateret.
Efterlevelse af instruks for behandling af personoplysninger ▶ Databehandler udfører alene behandling af personoplysninger, som fremgår af instruks fra dataansvarlig. ▶ Databehandleren har udarbejdet og implementeret skriftlige procedurer vedrørende behandling af personoplysninger, så der alene behandles efter instruks fra dataansvarlig. ▶ Databehandlerens procedurer gennemgås og opdateres løbende og minimum en gang årligt. ▶ Databehandleren udfører egenkontrol af efterlevelse af instruks i indgåede databehandleraftaler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens forståelseserklæring og observeret, at databehandleren alene udfører behandling af personoplysninger efter instruks fra dataansvarlig. Vi har inspiceret skabelon for databehandleraftale og observeret, at instruks fra dataansvarlig fremgår af databehandleraftalen. Vi har foretaget inspektion af at databehandleren har gennemgået procedurer i erklæringsperioden. Vi har foretaget inspektion af databehandlerens procedure for logning og overvågning og observeret, at databehandleren udfører egenkontrol for efterlevelse af instruks.	Ingen afvigelser konstateret.

Artikel 28, stk. 3 og 10, artikel 29 og artikel 32, stk. 4: Instruks for behandling af personoplysninger		
Kontrolmål ▶ *At sikre, at databehandleren alene handler efter dokumenteret instruks fra den dataansvarlige.* ▶ *At sikre, at databehandleren underretter den dataansvarlige, hvis en instruks er i strid med databeskyttelsesforordningen og databeskyttelsesloven.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Underretning af den dataansvarlige ved ulovlig instruks ▶ Databehandleren har udarbejdet en procedure for underretning af dataansvarlig, i tilfælde hvor den dataansvarliges instruks, strider mod databeskyttelseslovgivningen. ▶ Databehandleren underretter straks den dataansvarlige, i tilfælde hvor den dataansvarliges instruks strider mod databeskyttelseslovgivningen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure og har observeret, at denne indeholder retningslinjer for, at dataansvarlig skal underrettes i tilfælde af, at instruksen strider imod databeskyttelseslovgivningen. Vi har inspiceret skabelon for databehandleraftale og observeret, at det fremgår, at dataansvarlig skal underrettes straks, hvis instruksen strider imod databeskyttelseslovgivningen. Vi har på forespørgsel fået oplyst, at der ikke findes eksempler, hvor den dataansvarliges instruks strider mod databeskyttelseslovgivningen. Vi kan derfor ikke efterprøvet kontrollen.	Ingen afvigelser konstateret.

Artikel 28, stk. 2 og 4: Underdatabehandlere

Kontrolmål

- *At sikre, at underdatabehandleren er pålagt de samme databeskyttelsesforpligtelser, som databehandleren er pålagt af den dataansvarlige, ved indgåelse af en skriftlig kontrakt med tilhørende instruks.*
- *At sikre, at den dataansvarlige har givet en forudgående specifik eller generel skriftlig godkendelse af underdatabehandlere.*
- *At sikre, at underdatabehandleren kan stille de fornødne garantier til beskyttelse af personoplysningerne i overensstemmelse med kontrakten.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Underdatabehandleraftale og instruks ▶ Ved brug af underdatabehandler indgår databehandleren en databehandleraftale, der pålægger underdatabehandleren de samme databeskyttelsesforpligtelser, som databehandleren er pålagt. ▶ Instrukser fra dataansvarlig er videregivet til underdatabehandler. ▶ Databehandleraftalen med underdatabehandler underskrives og opbevares elektronisk.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens generiske aftale samt skabelon for databehandleraftale og observeret, at databehandleren pålægger underdatabehandleren de samme databeskyttelsesforpligtelser, som databehandleren er pålagt. Vi har for en stikprøve på en underdatadatabehandleraftale indgået med en underdatabehandler observeret, at databehandleren videregiver instruks fra den dataansvarlige til underdatabehandleren. Vi har foretaget inspektion af databehandlerens fildrev og har observeret, at underdatabehandleraftaler opbevares elektronisk.	Ingen afvigelser konstateret.
Godkendelse af underdatabehandlere ▶ Databehandler anvender kun godkendte underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens informationssikkerheds- og databeskyttelsespolitik og observeret, at databehandleren kun må anvende underdatabehandlere, på baggrund af en forudgående specifik eller generel skriftlig godkendelse, hos den dataansvarlige. Vi har foretaget inspektion af databehandlerens generiske aftale samt skabelon for databehandleraftale og observeret, at databehandleren ikke må anvende underdatabehandlere uden udtrykkelig skriftlig godkendelse fra den dataansvarlige.	Ingen afvigelser konstateret.

Artikel 28, stk. 2 og 4: Underdatabehandlere

Kontrolmål

- *At sikre, at underdatabehandleren er pålagt de samme databeskyttelsesforpligtelser, som databehandleren er pålagt af den dataansvarlige, ved indgåelse af en skriftlig kontrakt med tilhørende instruks.*
- *At sikre, at den dataansvarlige har givet en forudgående specifik eller generel skriftlig godkendelse af underdatabehandlere.*
- *At sikre, at underdatabehandleren kan stille de fornødne garantier til beskyttelse af personoplysningerne i overensstemmelse med kontrakten.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret skabelon på databehandleraftale og observeret, at databehandleren kun anvender en godkendt underdatabehandler og databehandleren får godkendelse til anvendelse af underdatabehandleren ved indgåelse af databehandleraftalen.	
Ændringer i godkendte underdatabehandlere ▶ Databehandler har udarbejdet en passende proces med dataansvarlig for udskiftning af godkendte underdatabehandlere. ▶ Databehandler underretter dataansvarlig ved udskiftning af underdatabehandler i forbindelse med generel godkendelse af underdatabehandler. ▶ Dataansvarlig har mulighed for at gøre indsigelse vedr. udskiftning af underdatabehandler. ▶ Ved udskiftning af underdatabehandler skal databehandleren have en ny forudgående specifik skriftlig godkendelse fra dataansvarlig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for aftaler og observeret, at databehandleren har udarbejdet en procedure for udskiftning af underdatabehandlere. Vi har inspiceret skabelon på databehandleraftale og observeret, at databehandleren har en proces for udskiftning af godkendte underdatabehandlere. Vi har på forespørgsel fået oplyst, at der ikke har været udskiftning af underdatabehandlere i erklæringsperioden, hvorfor vi ikke har kunnet efterprøve kontrollen.	Ingen afvigelser konstateret.
Oversigt over godkendte underdatabehandlere ▶ Databehandler har en oversigt over godkendte underdatabehandlere. Oversigt over godkendte underdatabehandlere indeholder blandt andet hvem der er kontaktperson, lokation for behandling samt hvilken type af behandling og kategori af personoplysninger, som underdatabehandler foretager.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens oversigt over underdatabehandlere og observeret, at databehandleren har udarbejdet en oversigt over godkendte underdatabehandlere, der indeholder informationer om kontaktperson, lokation for behandling samt type af behandling og kategori af personoplysninger.	Ingen afvigelser konstateret.

Artikel 28, stk. 2 og 4: Underdatabehandlere

Kontrolmål

- *At sikre, at underdatabehandleren er pålagt de samme databeskyttelsesforpligtelser, som databehandleren er pålagt af den dataansvarlige, ved indgåelse af en skriftlig kontrakt med tilhørende instruks.*
- *At sikre, at den dataansvarlige har givet en forudgående specifik eller generel skriftlig godkendelse af underdatabehandlere.*
- *At sikre, at underdatabehandleren kan stille de fornødne garantier til beskyttelse af personoplysningerne i overensstemmelse med kontrakten.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Tilsyn med underdatabehandlere ▶ Databehandleren udfører tilsyn med underdatabehandler. ▶ Databehandleren udfører tilsyn af underdatabehandleren baseret på en risikovurdering. ▶ Databehandler udfører tilsyn af underdatabehandler minimum en gang om året, baseret på en risikovurdering.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for tilsyn med underdatabehandlere og observeret, at denne anfører, at databehandleren skal udføre tilsyn med underdatabehandlere. Vi har foretaget inspektion af databehandlerens risikovurdering med underdatabehandleren og observeret, at databehandleren har udarbejdet en risikovurdering vedrørende risici hos underdatabehandleren. Vi har foretaget inspektion af databehandlerens procedure for tilsyn og observeret, at databehandleren skal føre tilsyn med underdatabehandlere én gang årlig. Vi har inspiceret, at databehandleren har foretaget tilsyn med underdatabehandleren via et kontrolbesøg hos Det Kongelige Bibliotek.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra b: Fortrolighed og lovbestemt tavshedspligt		
Kontrolmål ▶ *At sikre, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Tavsheds- og fortrolighedsaftale med medarbejdere ▶ Alle medarbejdere har underskrevet en databehandlerforståelseserklæring, der indeholder krav om tavshed og fortrolighed.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for styring af medarbejdere og observeret, at alle nye medarbejdere underskriver en tavsheds- og fortrolighedserklæring. Vi har foretaget inspektion af, at alle databehandlerens medarbejdere har underskrevet en databehandlerforståelseserklæring.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Risikovurdering ▶ Der foretages løbende og som minimum en gang årligt en risikovurdering af KOMDAs behandling af persondata baseret på potentielle risici for datas tilgængelighed, fortrolighed og integritet i forhold til den registreredes rettigheder og frihedsrettigheder. ▶ Sårbarheden af systemer og processer vurderes ud fra identificerede trusler. ▶ Risici minimeres ud fra vurderingen af deres sandsynlighed, konsekvens og afledte implementeringsomkostninger. ▶ Risikovurderinger opdateres løbende efter behov, men minimum en gang årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for risikovurdering og observeret, at risikovurderingen er vurderet i forhold til den registreredes rettigheder og frihedsrettigheder. Vi har foretaget inspektion af databehandlerens risikorapport og observeret, sårbarheden af systemer vurderes ud fra identificerede trusler. Vi har foretaget inspektion af databehandlerens risikorapport og observeret, risici minimeres ud fra vurderingen af deres sandsynlighed og konsekvens. Vi har foretaget inspektion af databehandlerens risikorapport og observeret, at denne er udarbejdet i februar 2023.	Ingen afvigelser konstateret.
Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse ▶ Databehandleren har etableret en beredskabsplan, der sikrer hurtig responstid til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse. ▶ Databehandleren har etableret periodisk afprøvning af beredskabsplanen med henblik på at sikre, beredskabsplanerne er tidssvarende og effektive i kritiske situationer.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens beredskabsplan og observeret, databehandleren har etableret en beredskabsplan, der sikrer hurtig responstid til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
▶ Beredskabstest dokumenteres og evalueres.	Vi har foretaget inspektion af skrivebordstest af beredskabsplanen og observeret, at denne er udført juni 2023.	
Opbevaring af personoplysninger ▶ Personoplysninger opbevares utilgængeligt for andre end de autoriserede. ▶ Adgang til personoplysninger tildeles på baggrund af arbejdsbetinget behov/need-to-know principper.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens politik for adgang til personoplysninger og observeret, at databehandleren har udarbejdet retningslinjer for brugerrettigheder og at adgang til oplysninger begrænses til personer med arbejdsbetinget behov. Vi har foretaget inspektion af tildeling af autorisationer og observeret, at tildeling er sket ud fra et arbejdsbetinget behov.	Ingen afvigelser konstateret.
Fysisk adgangskontrol ▶ Der er etableret fysiske adgangskontroller, som forebygger sandsynligheden for uautoriseret adgang til databehandlerens, faciliteter og personoplysninger, herunder sikring, af at kun autoriserede personer har adgang. ▶ Der foretages løbende og som minimum en gang om året gennemgang af den fysiske adgang til databehandlerens faciliteter.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for fysisk sikkerhed. Vi har foretaget inspektion af adgangsliste til serverrum og observeret, at det kun er KOMDA medarbejdere med et arbejdsbetinget behov, der har adgang.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har foretaget inspektion af databehandlerens procedure for nøgler og observeret, at databehandleren en gang årligt laver review af nøglefortegnelse.	

Fysisk sikkerhed
 	
- Der er etableret fysisk perimetersikring til at beskytte områder, der indeholder personoplysninger. Den fysiske perimetersikring er i overensstemmelse med de vedtagne sikkerhedskrav.
- Databehandleren har etableret kontroller til beskyttelse mod eksterne og miljømæssige trusler, herunder efterlevelse af specificerede krav til serverrum omfattende følgende forhold:
  - Gulve
  - Klima
  - Strøm
  - Adgang
  - Alarmmonitorering
  - Brandslukning
  - Kabling
	Vi har udført forespørgsel hos passende personale hos databehandleren.
	
	Vi har foretaget inspektion af databehandlerens procedure for fysisk sikkerhed.
	
	Vi har foretaget inspektion af databehandlerens serverrum og observeret, at databehandleren har etableret følgende kontroller til beskyttelse af data:
	
	- Vægge, gulve og loft er af brandhæmmende materialer.
	- Der er etableret system til styring af klima.
	- Der er etableret UPS, der kontrolleres hver måned.
	- Adgang til serverrum sker med særskilt nøgle.
	- Der er etableret røgalarm i serverrum samt skumslukker uden for serverrum.
	- Kabling er beskyttet
		Ingen afvigelser konstateret.

Logisk adgangskontrol - Databehandleren har implementeret procedure for brugeradministration der sikrer, at brugeroprettelser	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
og -nedlæggelser følger en styret proces, og at alle brugeroprettelser er autoriseret. ▶ Brugerrettigheder tildeles ud fra et arbejdsbetinget behov. ▶ Privilegerede (administrative) adgangsrettigheder tildeles til systemer og enheder ud fra arbejdsbetinget behov. ▶ Der foretages mindst en gang om året gennemgang af brugere og brugerrettigheder. ▶ Der foretages logning af alle adgange til systemer med persondata. ▶ Databehandleren har etableret logisk adgangskontrol til systemer med personoplysninger, herunder to-faktorautentifikation. ▶ Databehandleren har etableret regler for krav til adgangskoder, som skal følges af alle medarbejdere.	Vi har foretaget inspektion af databehandlerens procedure for autorisationer og observeret, at der er retningslinjer for brugeroprettelse og brugernedlæggelse. Vi har foretaget inspektion af tildelte autorisationer og observeret, at adgang er tildelt ud fra et arbejdsbetinget behov. Vi har foretaget inspektion af oversigt over autorisationer og observeret, at tildeling af privilegerede rettigheder, er tildelt ud fra et arbejdsbetinget behov. Vi har foretaget inspektion af databehandlerens gennemgang af autorisationer og observeret, at gennemgang er foretaget i perioden for revisionen. Vi har foretaget inspektion af skærmprint af log for adgang til ASDA og observeret, at der logges med navn og tidspunkt for adgang samt hvilken handling der er foretaget. Vi har foretaget inspektion af databehandlerens opsætning og observeret, at medarbejdere skal logge på med 2-faktor autentifikation. Vi har foretaget inspektion af databehandlerens informationssikkerheds- og databeskyttelsespolitik og observeret, at databehandleren har angivet retningslinjer for brug af passwords for medarbejdere.	

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Fjernarbejdspladser og fjernadgang til systemer og data ▶ Fjernadgang til databehandlerens systemer og data sker via en krypteret RDP-forbindelse. ▶ Fjernadgang skal foregå via to-faktor autentifikation	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af procedure for mobilt udstyr og fjernadgang og observeret, at der er angivet, at adgang skal ske via RDP og 2 faktorsikkerhed. Vi har foretaget inspektion af databehandlerens konfiguration af RDP-forbindelsen og observeret, at der er anvendt SSL (TLS 1.2) kryptering. Vi har foretaget inspektion af databehandlerens skærmprint af SMS Passcode indstillinger og observeret, at der skal anvendes 2-factor login, for at få adgang til data.	Ingen afvigelser konstateret.
Eksterne kommunikationsforbindelser ▶ Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall og RDP. ▶ Eksterne kommunikationsforbindelser er krypteret. ▶ Databehandleren har en oversigt over hvilke eksterne kommunikationsforbindelser der har tilladelse til at tilgå deres netværk.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af procedure for KOMDAs netværk, og observeret, at der er angivet at adgang til netværk sker via bestemte IP-ranges. Vi har for en stikprøve på en dataansvarlig observeret, at adgang er afgrænset i firewall til bestemt IP-adresse.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har foretaget inspektion af databehandlerens procedure for netværk og observeret, at databehandleren anvender RC8 (RDP standardkryptering). Vi har foretaget inspektion af opsætning af anvendt kryptering og observeret, at forbindelserne er krypteret i henhold til proceduren. Vi har foretaget inspektion af udtræk over eksterne kommunikationsforbindelser og observeret, at databehandleren har angivet, hvilke IP-ranges, der har tilladelse til at tilgå deres netværk.	
Kryptering af personoplysninger ▶ Databehandleren har implementeret en krypteringspolitik for kryptering af persondata. Politikken definerer styrken og protokollen for kryptering.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for netværksopsætning. Vi har foretaget inspektion af opsætning af kryptering og har observeret, at server med persondata er krypteret.	Ingen afvigelser konstateret.
Firewall ▶ Databehandler har konfigureret firewall korrekt efter best-practice-standard.	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
▶ Databehandler anvender kun services/porte som der er behov for. ▶ Firewalls er konfigureret og valideret periodisk efter behov.	Vi har foretaget inspektion af databehandlerens procedure for netværksopsætning. Vi har foretaget inspektion af opsætning af firewall og observeret, at content filter samt antivirus og IPS er slået til. Vi har foretaget inspektion af databehandlerens opsætning af firewall og observeret, at databehandleren har definerede regler for hvilke IP ranges, der er åbne. Vi har foretaget stikprøvevis inspektion af daglige rapporter fra firewall.	
Netværkssikkerhed ▶ Databehandleren anvender kendte netværksteknologier og mekanismer (Firewall/Intrusion Detection and Prevention System) for at beskytte internt netværk. ▶ Databehandlers netværk er segmenteret, og der er sat regler op mellem de enkelte segmenter, som gør, at der kun kan kommunikeres via få, udvalgte protokoller mellem segmenterne og ud til internettet.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens firewall opsætning og har observeret, at der er opsat scanning for inficerede filer i firewall. Vi har foretaget inspektion af databehandlerens procedure for netværk og observeret, at der anvendes adskilte netværk.	Ingen afvigelser konstateret.
Antivirusprogram ▶ Der er installeret antivirus-software på alle servere og arbejdsstationer og i Firewall'en.	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
▶ Antivirus-software opdateres løbende og opdateret med seneste version	Vi har foretaget inspektion af databehandlerens procedure for netværk og observeret, at der anførers, at der skal være installeret antivirus software på PC og servere. Vi har foretaget inspektion af opsætning af installeret antivirus software på PC og servere. Vi har foretaget inspektion af databehandlerens antivirus opsætning og observeret, at der sker løbende opdatering.	
Sårbarhedsscanning ▶ Databehandleren foretager sårbarhedsscanning eller penetrationstest af netværk efter behov. ▶ Databehandleren gennemgår inficerede filer i karantænemappen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for netværk og observeret, at denne anfører, at databehandleren skal foretage scanning af netværk efter behov. Vi er ved forespørgsel blevet oplyst, at databehandleren med baggrund i en risikovurdering har fravalgt at udføre en sårbarhedsscanning i erklæringsperioden. Vi har foretaget stikprøvevis inspektion af databehandlerens firewall rapport. Vi har foretaget inspektion af rapport fra firewall og observeret, at inficerede filer destrueres.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Sikkerhedskopiering og retablering af data ▶ Der udføres en test af, at data kan hentes fra underdatabehandler, mindst en gang årligt.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for dataoverførsel og observeret, at der skal udføres restore test en gang årligt. Vi har inspiceret dokumentation for, at databehandleren har gennemført en årlig restore test i erklæringsperioden.	Ingen afvigelser konstateret.
Vedligeholdelse af systemsoftware ▶ Operativsystem-software på servere og arbejdsstationer opdateres løbende. ▶ Databehandleren har implementeret en proces for opdatering af systemsoftware med henblik på at sikre systemers tilgængelighed og sikkerhed.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af procedure for KOMDAS netværk og observeret, at der er retningslinjer for opdatering af arbejdsstationer og servere. Vi har stikprøvevis foretaget inspektion af udtræk fra Windows patching af databehandlerens servere og observeret, at disse står til automatisk opdatering. Vi har foretaget inspektion af dokumentation for, at databehandleren foretager en månedlig kontrol af, at sikkerhedsopdateringerne er kørt.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger ▶ Alle succesfulde og mislykkede adgangsforsøg til databehandlerens systemer og data logges. ▶ Databehandler monitorerer og logger netværkstrafik. ▶ Databehandler opbevarer logs i maksimalt 6 måneder.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for logning og overvågning. Vi har foretaget inspektion af databehandlerens udtræk fra log over ASDA og observeret, at det fremgår, hvem der har tilgået systemet. Vi har inspiceret log fra Entrust samt fra ASDA og observeret, at databehandler har kontrolleret, at der ikke er data, der er ældre end 6 måneder.	Ingen afvigelser konstateret.
Overvågning ▶ Databehandleren notificeres om identificerede alarmer og følger op herpå.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for logning og overvågning. Vi har foretaget inspektion af log fra ASDA og fra Entrust og observeret, at databehandler notificeres ved alarmer og at der følges op herpå.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Bortskaffelse af it-udstyr ▶ Databehandleren bortskaffer it-udstyr ved fysisk destruktion af databærende medier.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af indgået aftale med firma vedrørende destruktion af it-udstyr. Vi har inspiceret, at destruktion af harddiske er sket via pågældende firma.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra g: Sletning og tilbagelevering af personoplysninger		
Kontrolmål ▶ *At sikre, at databehandleren kan slette og tilbagelevere personoplysninger, efter at tjenesten vedrørende behandlingen er ophørt, i henhold til instruks fra den dataansvarlige.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Sletning af personoplysninger ▶ Databehandleren sletter den dataansvarliges personoplysninger efter instruks, ved ophør af hovedaftalen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens informationssikkerheds- og databeskyttelsespolitik og observeret, at databehandleren sletter den dataansvarliges personoplysninger efter instruks, ved ophør af databehandleraftalen. Vi har på efterspørgsel fået oplyst, at der ikke har været ophør af databehandleraftale i erklæringsperioden.	Ingen afvigelser konstateret.
Tilbagelevering af personoplysninger ▶ Databehandleren tilbageleverer den dataansvarliges personoplysninger efter instruks, ved ophør af hovedaftalen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens informationssikkerheds- og databeskyttelsespolitik og observeret, at databehandleren tilbageleverer den dataansvarliges personoplysninger efter instruks, ved ophør af databehandleraftalen. Vi har på efterspørgsel fået oplyst, at der ikke har været ophør af databehandleraftaler i erklæringsperioden.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra e, f og h: Bistand til den dataansvarlige		
Kontrolmål ▶ *At sikre, at databehandleren kan bistå den dataansvarlige med opfyldelse af de registreredes rettigheder.* ▶ *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til behandlingssikkerhed (artikel 32), brud på persondatasikkerheden (artikel 33-34) og konsekvensanalyser (artikel 35-36).* ▶ *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til revision og inspektion.*		
Kontrolaktivitet	Test udført af BDO	Resultat af test
De registreredes rettigheder ▶ Databehandler har udarbejdet en procedure for bistand til dataansvarlige ved opfyldelse af de registreredes rettigheder. ▶ Det er muligt at give indsigt i alle oplysninger, der er registreret i ASDA.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens generiske aftale samt skabelon for databehandleraftale og observeret, at databehandleren forpligter sig til at bistå den dataansvarlige ved anmodninger om udøvelse af de registreredes rettigheder. Vi har på forespørgsel fået oplyst, at det er muligt at give indsigt i alle oplysninger, der er registreret i systemet via udtræk fra ASDA.	Ingen afvigelser konstateret.
Forpligtelser om behandlingssikkerhed, brud på persondatasikkerheden og konsekvensanalyser ▶ Der er udarbejdet procedurer for bistand til dataansvarlige ved opfyldelse af bistand i forhold til artikel 32-36.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens generiske aftale samt skabelon for databehandleraftale og observeret, at databehandleren forpligter sig til at bistå de dataansvarlige med disses forpligtelser efter databeskyttelsesforordningens art. 32-36. Vi har for en forespørgsel fra dataansvarlig vedrørende bistand i erklæringsperioden observeret, at databehandler har ydet bistand i forhold til opfyldelse af artikel 32-36.	Ingen afvigelser konstateret.
Revision og inspektion	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra e, f og h: Bistand til den dataansvarlige

Kontrolmål

- *At sikre, at databehandleren kan bistå den dataansvarlige med opfyldelse af de registreredes rettigheder.*
- *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til behandlingssikkerhed (artikel 32), brud på persondatasikkerheden (artikel 33-34) og konsekvensanalyser (artikel 35-36).*
- *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til revision og inspektion.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
▶ Databehandler kan få udarbejdet en ISAE 3000-erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger, rettet mod behandling og beskyttelse af personoplysninger. ▶ Databehandler bistår den dataansvarlige ved fysisk tilsyn ved at stille ressourcer til rådighed. ▶ Databehandleren stiller den fornødne information til rådighed for den dataansvarlige og tilsynsmyndigheden på anmodning i forbindelse med revision og inspektion af databehandleren.	Vi har foretaget inspektion af databehandlerens generiske aftale samt skabelon for databehandleraftale og observeret, at databehandleren forpligter sig til at få udarbejdet en revisorerklæring. Vi har udarbejdet nærværende ISAE 3000-erklæring til brug for databehandlerens forpligtelser i denne relation. Vi har foretaget inspektion af databehandlerens procedure for deltageres tilsyn med KOMDAs behandling af persondata og observeret, at databehandleren stiller alle nødvendige oplysninger til rådighed til bistand for den dataansvarlige ved revision og inspektion. Vi har på forespørgsel fået oplyst, at dataansvarlige eller Datatilsynet ikke har anmodet om fysisk tilsyn eller anden form for revision eller inspektion hos databehandleren i erklæringsperioden. Vi har derfor ikke kunne efterprøve kontrollen.	

Artikel 30, stk. 2, 3 og 4: Fortegnelse over kategorier af behandlingsaktiviteter

Kontrolmål

- *At sikre, at databehandleren udarbejder en skriftlig fortegnelse over alle kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige.*
- *At sikre, at databehandleren opbevarer fortegnelsen skriftligt, herunder elektronisk.*
- *At sikre, at databehandleren kan stille fortegnelsen til rådighed for tilsynsmyndigheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Fortegnelse over kategorier af behandlingsaktiviteter ▶ Databehandleren har etableret en fortegnelse over behandlingsaktiviteter som databehandler. ▶ Fortegnelsen opdateres løbende ved væsentlige ændringer. ▶ Fortegnelsen opdateres minimum en gang årligt under det årlige review.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens fortegnelse over behandlingsaktiviteter. Vi har foretaget inspektion af databehandlerens procedure for udarbejdelse af fortegnelse over behandlingsaktiviteter og observeret, at denne anfører, at databehandleren skal opdatere fortegnelsen efter behov. Vi har på forespørgsel fået oplyst, at der ikke har været ændringer til fortegnelsen i erklæringsperioden. Vi har derfor ikke kunne efterprøve kontrollen. Vi har foretaget inspektion af databehandlerens procedure og observeret, at der er foretaget review af procedure for fortegnelsen i erklæringsperioden.	Ingen afvigelser konstateret.
Opbevaring af fortegnelsen ▶ Fortegnelsen opbevares elektronisk i databehandlerens ESDH-system.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for udarbejdelse af fortegnelse over behandlingsaktiviteter og observeret, at databehandleren opbevarer fortegnelsen elektronisk. Vi har ved inspektion af proceduren observeret, at fortegnelsen opbevares elektronisk.	Ingen afvigelser konstateret.

Artikel 30, stk. 2, 3 og 4: Fortegnelse over kategorier af behandlingsaktiviteter		
Kontrolmål ▶ *At sikre, at databehandleren udarbejder en skriftlig fortegnelse over alle kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige.* ▶ *At sikre, at databehandleren opbevarer fortegnelsen skriftligt, herunder elektronisk.* ▶ *At sikre, at databehandleren kan stille fortegnelsen til rådighed for tilsynsmyndigheden.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Datatilsynets adgang til fortegnelsen ▶ Databehandleren udleverer fortegnelsen på anmodning fra Datatilsynet.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for udarbejdelse af fortegnelse over behandlingsaktiviteter og observeret, at databehandleren forpligter sig til at udlevere fortegnelsen på anmodning fra Datatilsynet. Vi har på forespørgsel fået oplyst, at Datatilsynet ikke har anmodet om få udleveret fortegnelsen i erklæringsperioden. Vi har derfor ikke kunne efterprøve kontrollen.	Ingen afvigelser konstateret.

Artikel 33, stk. 2: Underretning om brud på persondatasikkerheden

Kontrolmål

- *At sikre, at databehandleren uden unødig forsinkelse underretter den dataansvarlige om brud på persondatasikkerheden.*
- *At sikre, at den dataansvarlige underrettes om alle nødvendige oplysninger, så bruddet kan vurderes med henblik på anmeldelse til tilsynsmyndigheden og underretning til den registrerede.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Underretning om brud på persondatasikkerheden ▶ Databehandleren underretter den dataansvarlige om brud på persondatasikkerheden uden unødig forsinkelse. ▶ Databehandleren ajourfører den dataansvarlige med alle relevante og nødvendige oplysninger, når de er til rådighed for databehandleren. ▶ Kommunikation mellem databehandler og dataansvarlig dokumenteres og gemmes.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for registrering af brud på persondatasikkerheden og underretning af den dataansvarlige og observeret, at denne anfører, at databehandleren skal underrette den dataansvarlige om brud på persondatasikkerheden uden unødig forsinkelse. Vi har foretaget inspektion af databehandlerens skabelon for brud på persondatasikkerheden og observeret, at databehandleren følger en fast skabelon, som indeholder alle relevante oplysninger. Vi har foretaget inspektion af databehandlerens procedure for registrering af brud på persondatasikkerheden og underretning af den dataansvarlige og observeret, at denne anfører, at databehandleren skal dokumentere og gemme kommunikation mellem denne og den dataansvarlige. Vi har på forespørgsel fået oplyst, at der ikke har været brud på persondatasikkerheden i erklæringsperioden. Vi har derfor ikke kunne efterprøve kontrollen.	Ingen afvigelser konstateret.
Identifikation af brud på persondatasikkerheden ▶ Databehandleren har opsat overvågning af ASDA til detektion af brud på persondatasikkerheden. ▶ Databehandleren har udarbejdet en procedure for vurdering og identifikation af brud på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af databehandlerens procedure for registrering af brud. Vi har foretaget inspektion af log fra ASDA og observeret, at der logges for, hvilken handling der foretages.	Ingen afvigelser konstateret.

Artikel 33, stk. 2: Underretning om brud på persondatasikkerheden		
Kontrolmål ▶ *At sikre, at databehandleren uden unødig forsinkelse underretter den dataansvarlige om brud på persondatasikkerheden.* ▶ *At sikre, at den dataansvarlige underrettes om alle nødvendige oplysninger, så bruddet kan vurderes med henblik på anmeldelse til tilsynsmyndigheden og underretning til den registrerede.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har foretaget inspektion af log fra Entrust og observeret, at der logges for uautoriseret adgang. Vi har på forespørgsel fået oplyst, at der ikke har været brud på persondatasikkerheden i erklæringsperioden. Vi har derfor ikke kunne efterprøve kontrollen.	

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

KYSTVEJEN 29
8000 AARHUS C

CVR-NR. 20 22 26 70

BDO Statsautoriseret revisionsaktieselskab, danskejet rådgivnings- og revisionsvirksomhed, er medlem af BDO International Limited - et UK-baseret selskab med begrænset hæftelse - og del af det internationale BDO netværk bestående af uafhængige medlemsfirmaer. BDO er varemærke for både BDO netværket og for alle BDO medlemsfirmaerne. BDO i Danmark beskæftiger mere end 1.500 medarbejdere, mens det verdensomspændende BDO netværk har ca. 90.000 medarbejdere i mere end 167 lande.