Staten og Kommunernes Indkøbsservice

ISAE 3000-erklæring fra uafhængig revisor vedrørende procedurer og kontroller etableret til beskyttelse af persondata i indkøbsdatasamarbejdet

pr. 17. februar 2020

Building a better working world

Indhold

1 Serviceleverandørens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for de kunder, der har indkøbsdatasamarbejde hos Staten og Kommunernes Indkøbsservice (SKI), og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne selv har anvendt, så de opnår en forståelse af kundernes informationssystemer.

Denne erklæring er udarbejdet i henhold til partielmetoden for så vidt angår underleverandørerne Atea, ProAct, KMD og Microsoft. Vores beskrivelse omfatter således ikke kontrolmål og tilknyttede kontroller hos disse underleverandører.

SKI bekræfter, at:

(a) den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af indkøbsdatasamarbejdet, der behandler fakturadata pr. 17. februar 2020. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

  (i) redegør for, hvordan systemet var udformet og implementeret, herunder redegør for:

    - de typer af ydelser, der er leveret, herunder behandlede grupper af transaktioner, når det er relevant
    - de processer i både it-systemer og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere transaktionerne samt overføre disse til de rapporter, der er udarbejdet til kunder
    - hvordan systemet behandlede andre betydelige begivenheder og forhold end transaktioner
    - processen, der blev anvendt til at udarbejde rapporter til kunder
    - relevante kontrolmål og kontroller udformet til at nå disse mål
    - kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementeret af brugervirksomhederne, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå
    - andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen og rapporteringen af kunders transaktioner.

  (ii) ikke udelader eller forvansker information, der er relevant for omfanget af det beskrevne system, under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved systemet, som den enkelte kunde måtte anse for vigtigt efter deres særlige forhold.

(b) de kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. 31. december 2019. Kriterierne for denne udtalelse var, at:

  (i) de risici, som truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret, og

  (ii) de identificerede kontroller ville, hvis anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrer opnåelsen af de anførte kontrolmål.

København, den 17. marts 2020
Staten og Kommunernes Indkøbsservice

Jonas Klinting
Økonomidirektør

2 Serviceleverandørs uafhængige revisors erklæring med sikkerhed om beskrivelsen af kontroller og deres udformning

Til: Staten og Kommunernes Indkøbsservice

Omfang

Vi har fået som opgave at afgive erklæring om Staten og Kommunernes Indkøbsservices (SKI) beskrivelse i afsnit 3 om indkøbsdatasamarbejdet og behandlingen af kunders fakturadata pr. 17. februar 2020 (beskrivelsen) og om udformningen af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vi har ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

Ledelsens beskrivelse af forretningskontrollerne omfatter alene kontrolmål og tilknyttede kontroller hos SKI. Generelle it-kontroller udført hos Atea, ProAct, KMD og Microsoft er udeladt. Vores handlinger omfatter således ikke kontrolmål og tilknyttede kontroller hos disse underleverandører

Denne erklæring er udarbejdet i henhold til partielmetoden vedrørende Atea, ProAct, KMD og Microsoft.

Enkelte af de kontrolmål, der er anført i SKI's beskrivelse af indkøbsdatasamarbejdet, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos SKI. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementerende kontroller.

SKI's ansvar

SKI er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter; for at anføre kontrolmålene; samt for udformningen, implementeringen og effektivt fungerende kontroller for at nå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i IESBA's Etiske regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

Vi anvender ISQC 1 og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

Serviceleverandørens revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om SKI's beskrivelse samt om udformningen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3000, andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger, som er udstedt af IAASB, og yderligere krav ifølge dansk revisorlovgivning. 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.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes udformning. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet.

En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål og hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet i afsnit 1.

Som nævnt ovenfor har vi ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

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

Begrænsning i kontroller hos en serviceleverandør

SKI's beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som hver enkelt kunde måtte anse for vigtigt efter deres særlige forhold.

Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner.

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 afsnit 1. Det er vores opfattelse, at:

(a) beskrivelsen af indkøbsdatasamarbejdet, således som det var udformet og implementeret pr. 17. februar 2020, i alle væsentlige henseender er retvisende, og

(b) kontrollerne, der knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 17. februar 2020.

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt de kommuner, der deltager i indkøbsdatasamarbejdet hos SKI, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kundens egne kontroller.

Frederiksberg, den 17. marts 2020
ERNST & YOUNG
Godkendt Revisionspartnerselskab
CVR-nr. 30 70 02 28

Nils B. Christiansen
statsaut. revisor
mne34106

3 Systembeskrivelse

3.1 Introduktion

Det fælleskommunale indkøbsdatasamarbejde har til formål at styrke kommunernes grundlag for at effektivisere indkøbsområdet ved løbende at indsamle, analysere og formidle kommunale indkøbsdata ud fra kommunernes købsfakturaer.

3.2 Juridisk struktur

Staten og Kommunernes Indkøbsservice A/S (SKI) er ejet af Finansministeriet og kommunerne via KL med henholdsvis 55 % og 45 %. SKI har som overordnet formål at effektivisere og professionalisere de offentlige indkøb, hvilket blandt andet indebærer at skabe viden omkring offentligt indkøb. SKI er operatør på indkøbsdatasamarbejdet og forestår indsamlingen og analyserne.

3.3 Beskrivelse af indkøbsdatasamarbejdet

I forbindelse med indkøbsdatasamarbejdet indsamles de deltagende kommuners købsfakturaer for perioden 2014-2018 i årene 2017-2019. I praksis indebærer det, at kommunerne skal overføre en kopi af deres elektroniske fakturadata til indkøbsdatasamarbejdet.

For at kategorisere e-fakturaerne - dvs. oversætte den enkelte fakturalinje til en indkøbskategori såsom "Kuglepenne" eller "Aftørringspapir" - har SKI for den ovenfor nævnte periode indgået en aftale med KMD, der fungerer som underleverandør. KMD kategoriserer e-fakturaerne og sender de kategoriserede e-fakturaoplysninger retur til SKI.

Alle SKI's analyser foretages på baggrund af de kategoriserede e-fakturaoplysninger (analysedata), og der udarbejdes individuelle rapporter for alle de deltagende kommuner, som herefter udsendes til kommunerne.

3.4 Beskrivelse af dataudveksling

Kommunerne kan bidrage med deres fakturadata på to forskellige måder. Kommunerne kan uploade deres fakturadata til SKI til en sikret krypteret server. SKI vil herefter gemme de oprindelige fakturaer, som kommunerne har uploadet, og udbygger derved denne samling, i takt med at de deltagende kommuner fremover sender nye års e-fakturadata til SKI. Det vil sikre, at SKI fremover fx kan skifte underleverandør til kategoriseringsopgaven, uden at dette kræver, at alle de deltagende kommuner på ny skal fremsende flere års fakturaer til SKI.

Den anden måde, kommunerne kan deltage på, omfatter de kommuner, der anvender KMD Indkøbsanalyse. I forlængelse af SKI's aftale med KMD om kategoriseringsaftalen er der indgået en aftale, der betyder, at såfremt en kommune har en aftale med KMD om anvendelse af KMD Indkøbsanalyse, kan kommunen vælge at overføre dens fakturadata til indkøbsdatasamarbejdet vederlagsfrit. Det betyder, at kommunens data kan overføres til samarbejdet uden separat udtræk og upload til SKI. Kommunen skal alene udarbejde og sende en instruks, der giver KMD lov til at overføre fakturadata til indkøbsdatasamarbejdet.

Uafhængigt af dataudvekslingsmetode gælder det, at SKI gemmer de modtagne data i op til 5 år efter modtagelsen, hvorefter de slettes. Det vil konkret betyde, at fakturadata for perioden 2014-2016, som SKI modtog i foråret 2017, vil blive slettet senest i foråret 2022. Fakturadata, som SKI modtager i foråret 2018, vil tilsvarende blive slettet senest i foråret 2023 og så fremdeles.

3.5 Definering af dataansvar/ databehandler

SKI har med hver enkelt deltagende kommune indgået en databehandleraftale, der bl.a. redegør for forhold omkring indsamling, opbevaring, bearbejdning samt efterfølgende sletning af kommunernes data.

SKI er dermed databehandler i forhold til hver enkelt kommune, der til gengæld fungerer som dataansvarlig med hensyn til de pågældende data.

3.6 Beskrivelse af erklæringens omfang

Nærværende erklæring baserer sig alene på kontroller i SKI's eget regi. Dermed er der ikke set på kontrolmål og kontroller hos SKI's backupleverandører Atea og ProAct, underdataleverandøren KMD, som kategoriserer fakturadata, samt eventuelle cloud-baserede underleverandører (Microsoft).

3.7 Risikostyring

De indsamlede fakturaer kan for fås vedkommende og i begrænset omfang indeholde personoplysninger såsom:

- Navn, fødselsdato og CPR-numre.
- Oplysninger om stilling, e-mail, adresser og øvrige kontaktoplysninger.
- Oplysninger om ansættelsesforhold.
- Enkeltstående tilfældighedsprægede oplysninger om de berørte borgere m.v., som er genstand for leverancerne, som herunder indirekte eller direkte kan omfatte fx helbredsmæssige oplysninger, oplysninger af privat karakter. Disse behandles alene som led i bortfiltrering hos SKI ved dannelse af analysegrundlaget ud fra fakturaerne.

SKI har i aftalen med underdatabehandleren KMD aftalt en procedure, som har til formål at erstatte CPR-numre med en generisk beskrivelse. Denne procedure har fjernet størstedelen af CPR-numrene. Yderligere er denne procedure skærpet i de seneste dataleverance (for fakturaårene 2017 og 2018) fra KMD til SKI. Uden at fange alle personoplysninger anonymiserer den skærpede procedure også personnavne, fysiske adresser, telefonnumre og mailadresser.

Kun et begrænset antal ansatte i SKI har adgang til de kategoriserede fakturadata til behandlingsformål. De pågældende ansatte, der behandler data, er underlagt procedurer, som har til formål bl.a. at sikre, hvordan data, der selv efter anonymiseringsprocessen indeholder personhenførbare oplysninger, behandles.

3.8 Beskrivelse af procedure, der skal udføres af kommunerne

SKI har i sin vejledning til kommunerne beskrevet, hvordan dataflowet mellem kommunerne og SKI skal foregå med henblik på en sikker håndtering af personoplysninger. Gennem anvendelse af en sikret server hos SKI m.v. er det muligt for kommunerne at sende deres fakturadata krypteret til SKI. Det forudsættes dermed fra SKI's side, at kommunerne overholder de udsendte vejledninger om fremsendelse af data. SKI forudsætter endvidere, at kommunernes interne procedurer omkring modtagelse og håndtering af fortroligheden vedrørende sikker post følges korrekt.

3.9 Beskrivelse af procedurer og kontroller

3.9.1 Generelle sikkerhedsbestemmelser

Kontrolmål: Kontroller giver rimelig grad af sikkerhed for, at der er implementeret sikkerhedsforanstaltninger, der stemmer overens med databehandleraftalen.

SKI har etableret en sikkerhedsfunktion med ansvarsområdet it-sikkerhed og fysisk sikkerhed på SKI's lokation. På SKI's lokation er der etableret fysiske adgangsforhold, der sikrer, at kun ansatte hos SKI har adgang til de indkøbsdata, der behandles, herunder at kun få autoriserede medarbejdere har adgang til den server, hvor indkøbsdata opbevares. SKI har etableret procedurer for godkendelse, tildeling og periodisk gennemgang af adgangsrettigheder, der er implementeret i hele SKI-organisationen (1.1a).

SKI har udarbejdet generelle retningslinjer for informationssikkerhed, der fastlægger ansvaret for anvendelse af edb-udstyr. Yderligere har SKI udarbejdet procedurer, som fastlægger ansvaret for og beskriver behandling af ind- og uddatamateriale, således er der udarbejdet dokumentation for sletning af testdata samt underdataleverandørens (KMD) sletteproces (1.1b).

I SKI's generelle retningslinjer for informationssikkerhed er der fastlagt retningslinjer for den generelle sikkerhedspolitik i SKI. Disse retningslinjer gennemgås i henhold til årshjulet (1.1c) (1.2).

SKI's generelle retningslinjer for informationssikkerhed indeholder retningslinjer for fjernarbejdspladser, herunder krav om, at adgangen til SKI's systemer sker via krypteret VPN-forbindelse (1.3). Dog har SKI en række formelle retningslinjer for fjernarbejdspladser (1.3a).

I forbindelse med salg, genbrug og kassation samt reparation af anvendt it-udstyr er der fastlagt procedurer og retningslinjer for informationssikkerhed (1.4) (1.5).

3.9.2 Inddatamateriale, som indeholder personoplysninger

Kontrolmål: Kontroller giver rimelig grad af sikkerhed for, at inddatamateriale er beskyttet og kun kan tilgås af autoriserede brugere, samt at inddatamaterialet slettes i henhold til frister anført i databehandleraftalen.

Inddatamaterialet kan kun tilgås af et begrænset antal medarbejdere i SKI. Dette er fastlagt i dokumentet procesdokumentation for indkøbssystem. Alt inddatamateriale er elektronisk og er placeret på sikrede krypterede servere (2.1).

SKI har endnu ikke slettet produktionsdata leveret til samarbejdet. Dog er der etableret en procedure for sletningen, som har været anvendt i forbindelse med testdata vedrørende nærværende indkøbsdatasamarbejde og i forbindelse med tidligere pilotprojekt (2.2).

SKI er ifølge databehandleraftalen senest 5 år efter modtagelsen forpligtet til at slette de kommunale fakturadata. Denne frist er ikke overskredet. Yderligere giver databehandleraftalen den dataansvarlige mulighed for at anmode om at slette. Dette er ved erklæringens udarbejdelse endnu ikke sket. Der er udarbejdet procedure for sletning (2.2a).

3.9.3 Autorisation og adgangskontrol

Kontrolmål: Kontroller giver rimelig grad af sikkerhed for, at adgang til behandling af indkøbsdata er begrænset og kun kan udføres af autoriserede brugere.

Der er fastlagt retningslinjer for, hvilke personer der kan få adgang til behandlingen af indkøbsdata indeholdende personoplysninger. Yderligere er der fastlagt en retningslinje for, hvordan nye medarbejdere får adgang til data, ligesom der er retningslinjer for fjernelse af adgangen for fratrådte medarbejdere (3.1). Adgangen til data er ikke styret af roller, men udelukkende om der er adgang til data eller ej (3.2). Formålet med indkøbsdatasamarbejdet er at skabe viden og statistik i form af rapporter til de tilsluttede kommuner samt input til udvikling af nye rammeaftaler (3.3). Ud over den begrænsede personkreds med adgang til behandling af personoplysninger har også SKI's interne og eksterne drifts- og systemteknikere samt revision adgang til indkøbsdata (3.3a). Kontrollen af adgangen til indkøbsdata indgår i årshjulet (3.4) (3.5).

3.9.4 Kontrol med afviste adgangsforsøg

Kontrolmål: Kontroller giver rimelig grad af sikkerhed for, at brugeradgang afvises og spærres ved gentagne afviste adgangsforsøg.

SKI's it-system registrerer gentagne afviste adgangsforsøg, og kontoen udelukkes indtil SKI's it-afdeling aktivt åbner for den igen. Yderligere fremsendes der en systemgenereret mail til SKI's it-afdeling om udelukkelsen (4.1).

3.9.5 Uddatamateriale, som indeholder personoplysninger

Kontrolmål: Kontroller giver rimelig grad af sikkerhed for, at uddatamateriale er beskyttet og kun kan tilgås af autoriserede brugere, samt at uddatamaterialet slettes i henhold til frister anført i databehandleraftalen.

For at imødekomme sikkerheden har SKI udarbejdet procedurer, der har til formål at sikre en korrekt behandling og håndtering af personoplysninger. Som udgangspunkt udarbejdes udelukkende rapporter og andet uddatamateriale, der ikke indeholder personoplysninger. I de få tilfælde, hvor der indgår personoplysninger, renses disse både maskinelt (se 3.7) og manuelt ud inden videregivelse. Uddatamateriale indeholdende personoplysninger sendes udelukkende via sikker post eller via en krypteret OneDrive-adgang, hvortil en bestemt ekstern bruger kan tildeles adgang (5.1). Ud over den begrænsede personkreds har også SKI's interne og eksterne drifts- og systemteknikere samt revision adgang til uddatamateriale indeholdende personoplysninger (5.1a). Uddatamateriale gemmes på krypterede servere på SKI's

fysiske adresse, hvor der kræves separat adgangstilladelse (5.2). Uddatamateriale er endnu ikke blevet tilintetgjort, idet fristen endnu ikke er overskredet, eller at en kommune har anmodet om at få uddata slettet. Imidlertid er der udarbejdet en procedure omkring sletning af uddatamateriale omhandlende enkeltpersoner eller en enkelt kommunes samlede data (5.3). Ud over ovenstående er SKI's generelle it-sikkerhedspolitik implementeret med passende tekniske og organisatoriske foranstaltninger (5.4). I de tilfælde, hvor kommunen anmoder om sit eget fuldt kategoriserede datasæt, er rensningen af personoplysninger udelukkende baseret på den maskinelle metode. Data sendes til den kontaktperson, som kommunen selv har udpeget til samarbejdet via en krypteret forbindelse.

3.9.6 Eksterne kommunikationsforbindelser

Kontrolmål: Kontroller giver rimelig grad af sikkerhed for, at eksterne kommunikationsforbindelser er sikret.

I forbindelse med håndtering af personoplysninger anvendes følgende eksterne kommunikationsforbindelser; VPN ved fjernarbejdspladser, krypterede servere, sikker post ved uddata med personoplysninger og anvendelse af OneDrive-adgang. Fællesnævneren for disse er, at der er tale om krypterede forbindelser, der skal sikre, at uvedkommende ikke får adgang til data (6.1).

3.9.7 Logning

Kontrolmål: Kontroller giver rimelig grad af sikkerhed for, at brugen af fakturadata logges.

Alle søgninger i fakturadata logges. Der skelnes i denne forbindelse ikke mellem persondata eller ej persondata (7.1). Denne logning består af brugernavn, tidspunkt og søgekriterier. (7.1a) Hvis en kommune eller tilsynsmyndighed ønsker at modtage kopi af logfilen, er der oprettet procedure herfor (7.2).

4 Tests udført af EY

4.1 Formål og omfang

Vores arbejde blev gennemført i overensstemmelse med ISAE 3000, andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger (andre erklæringsopgaver med sikkerhed).

Vores test af kontrollernes udformning har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår af afsnit 4.3. Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos regioner/kommuner er ikke omfattet af vores gennemgang.

Vores test har omfattet de kontroller, der er knyttet til de kontrolmål, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de specifikke kontrolmål er opfyldt pr. 17. februar 2020.

4.2 Udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers udformning og effektivitet er beskrevet nedenfor.

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er udformet og implementeret, så de kan forventes at blive effektive. Endvidere har vi vurderet, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Forespørgsler	Forespørgsel af passende personale hos SKI. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Vi har observeret udførelsen af kontrollen.
Genudførelse	Vi har observeret kontrollens udførelse og implementering med henblik på at verificere, at kontrollen har fungeret som forudsat.

4.3 Resultater af tests

Kontrolmål – Generelle sikkerhedsbestemmelser
1. Kontroller giver rimelig grad af sikkerhed for, at der er implementeret sikkerhedsforanstaltninger, der stemmer overens med databehandleraftalen.

#	Kontrolaktivitet	Udførte tests	Resultater af tests udført af EY
1.1a	Databehandleren skal fastsætte interne bestemmelser om sikkerhedsforanstaltninger til uddybning af de krav, der fremgår af dette bilag. Bestemmelserne skal navnlig omfatte organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer.	Forespurgt til sikkerhedsorganisationen hos SKI. Forespurgt til fysisk sikring hos SKI. Forespurgt til administration af adgange og autorisationer. Inspiceret administration af fysiske adgangsforhold for adgange til databehandlingsfaciliteter. Inspiceret administration af autorisationer til databehandlingsfaciliteter. Inspiceret oversigt over fysiske nøgler.	Ingen afvigelser konstateret.
1.1b	Databehandleren skal fastsætte interne bestemmelser om sikkerhedsforanstaltninger til uddybning af de krav, der fremgår af dette bilag. Der skal fastsættes instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af edb-udstyr.	Forespurgt til procedure for sletning af ind- og ud datamateriale. Inspiceret informationssikkerhedspolitikken. Inspiceret dokumentation for datasletning. Inspiceret erklæring for sletning af data leveret til SKI-Dataprojekt 2019 hos KMD A/S.	Ingen afvigelser konstateret.
1.1c	Databehandleren skal fastsætte interne bestemmelser om sikkerhedsforanstaltninger til uddybning af de krav, der fremgår af dette bilag. Der skal fastsættes retningslinjer for tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for Databehandleren.	Forespurgt til tilsyn med overholdelse af sikkerhedsforanstaltningerne. Inspiceret retningslinjer for informationssikkerhed.	Ingen afvigelser konstateret.

#	Kontrolaktivitet	Udførte tests	Resultater af tests udført af EY
1.2	De interne bestemmelser skal gennemgås mindst én gang årligt med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold hos Databehandleren.	Forespurgt til procedure for årlig gennemgang af sikkerhedsbestemmelserne. Inspiceret informationssikkerhedspolitisk status 2019. Inspiceret ledelsesgodkendt informationssikkerhedspolitik. Inspiceret årlig gennemgang af interne bestemmelser.	Ingen afvigelser konstateret.
1.3	Databehandleren skal fastsætte særlige retningslinjer for behandling af personoplysninger omfattet af Databehandleraftalen, der finder sted på en arbejdsplads uden for Databehandlerens lokaliteter (fjernarbejdsplads), således at det sikres, at de fornødne tekniske og organisatoriske foranstaltninger iagttages i relation til denne behandling af oplysningerne.	Forespurgt til procedure for fjernarbejdspladser. Inspiceret retningslinjer for fjern- og hjemmearbejdspladser. Observeret brugen af VPN. Inspiceret dokumentation for opsætning af VPN og dens krypteringsniveau.	Ingen afvigelser konstateret.
1.3a	Såfremt behandlingen af personoplysninger hos Databehandleren sker helt eller delvist ved anvendelse af hjemmearbejdspladser, skal Databehandleren fastsætte retningslinjer for medarbejdernes behandling af personoplysninger ved anvendelse af hjemmearbejdspladser.	Forespurgt til procedure for fjernarbejdspladser. Inspiceret retningslinjer for fjern- og hjemmearbejdspladser. Observeret brugen af VPN. Inspiceret dokumentation for opsætning af VPN og dens krypteringsniveau.	Ingen afvigelser konstateret.

#	Kontrolaktivitet	Udførte tests	Resultater af tests udført af EY
1.4	I forbindelse med salg, genbrug og kassation af anvendt udstyr, herunder dataudstyr og datamedier, der indeholder personoplysninger omfattet af Databehandleraftalen, og som har været anvendt til Databehandleraftalens opfyldelse, skal Databehandleren træffe passende tekniske og organisatoriske foranstaltninger for at sikre, at disse oplysninger hverken hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt træffe foranstaltninger mod, at disse personoplysninger kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med de persondataretlige regler og/eller denne Databehandleraftale.	Inspiceret retningslinjer for informationssikkerhed, genbrug, destruktion og reparation af udstyr. Inspiceret dokumentation for kryptering af datamedier.	Ingen afvigelser konstateret.
1.5	I forbindelse med reparation og service af udstyr, der anvendes til opfyldelse af formålene med behandlingen af oplysninger omfattet af Databehandleraftalen, og som indeholder oplysninger omfattet af Databehandleraftalen, skal Databehandleren træffe de fornødne foranstaltninger for at sikre, at oplysningerne hverken hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt foranstaltninger mod, at oplysningerne kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med de persondataretlige regler eller denne Databehandleraftale.	Inspiceret retningslinjer for informationssikkerhed, genbrug, destruktion og reparation af udstyr. Inspiceret dokumentation for kryptering af datamedier.	Ingen afvigelser konstateret.

Kontrolmål – Inddatamateriale som indeholder personoplysninger
2. Kontroller giver rimelig grad af sikkerhed for, at inddatamateriale er beskyttet og kun kan tilgås af autoriserede brugere, samt at inddatamaterialet slettes i henhold til frister anført i databehandleraftalen.

#	Kontrolaktivitet	Udførte tests	Resultater af tests udført af EY
2.1	Databehandleren skal sikre, at inddatamateriale indeholdende personoplysninger omfattet af Databehandleraftalen kun anvendes af personer, som er beskæftiget med inddatering i forbindelse med opfyldelse af formålene med behandlingen af oplysninger omfattet af Databehandleraftalen. Inddatamaterialet skal opbevares aflåst, når det ikke anvendes.	Forespurgt til procedurer for behandling af inspiceret indkøbsdatasamarbejde i SKI. Inspiceret procedure for oprettelse og nedlæggelse af brugeradgange. Inspiceret dokumentation for gennemgang af brugeradgange.	Ingen afvigelser konstateret.
2.2	Inddatamateriale skal slettes eller tilintetgøres, når det ikke længere skal anvendes til formålene med behandlingen af oplysninger omfattet af Databehandleraftalen eller til kontrol med de inddaterede personoplysninger, dog senest efter en af den Dataansvarlige nærmere fastsat frist.	Forespurgt til procedure for sletning af inddatamateriale. Inspiceret dokumentation for datasletning. Inspiceret erklæring for sletning af data leveret til SKI-Dataprojekt 2019 hos KMD A/S.	Ingen afvigelser konstateret.
2.2a	Ved tilintetgørelse af inddatamaterialet træffer Databehandleren de fornødne sikkerhedsforanstaltninger mod, at materialet misbruges eller kommer til uvedkommendes kendskab.	Forespurgt til procedure for sletning af inddatamateriale. Inspiceret dokumentation for datasletning. Inspiceret erklæring for sletning af data leveret til SKI-Dataprojekt 2019 hos KMD A/S.	Ingen afvigelser konstateret.

Kontrolmål – Autorisation og adgangskontrol
3. Kontroller giver rimelig grad af sikkerhed for, at adgang til behandling af indkøbsdata er begrænset og kun kan udføres af autoriserede brugere.

#	Kontrolaktivitet	Udførte tests	Resultater af tests udført af EY
3.1	Databehandleren skal sikre, at kun de personer, som autoriseres hertil, må have adgang til personoplysninger, der behandles efter aftalen.	Forespurgt til tildeling af adgangsrettigheder vedrørende indkøbsdatasamarbejdes projektet. Inspiceret dokumentation for tildelte adgange til data i indkøbsdatasamarbejdet. Inspiceret procedure samt dokumentation for oprettelse af adgange til datasamarbejdsprojektet.	Ingen afvigelser konstateret.
3.2	Databehandleren skal sikre, at Databehandlerens medarbejdere autoriseres og tildeles rettigheder i overensstemmelse med Databehandlerens interne retningslinjer efter punkt 1, hvori det er beskrevet, i hvilket omfang Databehandlerens medarbejdere må forespørge på, inddatere eller slette oplysninger omfattet af Databehandleraftalen.	Forespurgt til proceduren for tildeling af rettigheder. Inspiceret dokumentation for oprettelses- og nedlæggelsesprocedurer af adgange til indkøbsdatasamarbejdet.	Vi er blevet oplyst om, at der ikke har været til- eller fratrædelser af medarbejdere tilknyttet indkøbsdatasamarbejdet. Ingen afvigelser konstateret.
3.3	Databehandleren må kun autorisere personer, der er beskæftiget med de formål, hvortil personoplysninger behandles i forbindelse med Databehandleraftalens opfyldelse. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har specifikt behov for i forbindelse med Aftalens opfyldelse.	Forespurgt til medarbejderes arbejdsbetingede behov for behandling af data fra indkøbsdatasamarbejdet. Inspiceret procedure samt dokumentation for oprettelse af adgange til datasamarbejdsprojektet. Inspiceret dokumentation for tildelte adgange til data i indkøbsdatasamarbejdet.	Ingen afvigelser konstateret.

#	Kontrolaktivitet	Udførte tests	Resultater af tests udført af EY
3.3a	Ud over det i forrige afsnit angivne må Databehandleren endvidere autorisere brugere, for hvem adgang til oplysningerne er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver i forbindelse med opfyldelse af formålene med behandlingen af personoplysningerne.	Inspiceret dokumentation for, at privilegerede adgange til indkøbsdatasamarbejdet er begrænset og godkendt.	Ingen afvigelser konstateret.
3.4	Databehandleren skal som minimum træffe de foranstaltninger, der er beskrevet i Databehandlerens interne retningslinjer efter punkt 1 for at sikre, at kun autoriserede brugere kan få adgang, og at disse kun kan få adgang til de oplysninger og anvendelser, som de er autoriserede til i forbindelse med Databehandleraftalens opfyldelse.	Forespurgt til medarbejderes arbejdsbetingede behov for behandling af data fra indkøbsdatasamarbejdet. Inspiceret dokumentation for tildelte adgange til data i indkøbsdatasamarbejdet.	Ingen afvigelser konstateret.
3.5	Databehandleren skal løbende sikre og dokumentere, at de autoriserede brugere fortsat opfylder betingelserne i punkt 4 og Databehandlerens interne retningslinjer efter punkt 1. Kontrol heraf skal foretages mindst én gang hvert halve år.	Forespurgt til medarbejderes arbejdsbetingede behov for behandling af data fra indkøbsdatasamarbejdet. Forespurgt til proceduren for gennemgang af brugeradgange. Inspiceret dokumentation for gennemgang af brugeradgange.	Ingen afvigelser konstateret.

Kontrolmål – Kontrol med afviste adgangsforsøg
4. Kontroller giver rimelig grad af sikkerhed for, at der foretages registrering af adgangsforsøg, og afviste adgangsforsøg udløser en blokering af brugeren.

#	Kontrolaktivitet	Udførte tests	Resultater af tests udført af EY
4.1	Databehandleren skal foretage registrering af og dokumentere alle afviste adgangsforsøg. Hvis der inden for en af den Dataansvarlige bestemt periode er registreret et af den Dataansvarlige bestemt antal på hinanden følgende afviste adgangsforsøg fra samme arbejdsstation eller med samme brugeridentifikation, skal der blokeres for yderligere forsøg. Databehandleren skal løbende afrapportere herom til den Dataansvarlige.	Inspiceret opsætning for maksimum antal loginforsøg. Observeret, at en bruger bliver lukket efter 10 forkerte loginforsøg. Observeret, at it skal åbne brugeren, før den kan benyttes igen. Forespurgt til rapportering om afviste loginforsøg.	Ingen afvigelser konstateret.

Kontrolmål – Uddatamateriale, som indeholder personoplysninger
5. Kontroller giver rimelig grad af sikkerhed for, at uddatamateriale indeholdende personoplysninger behandles på fortrolig og hensigtsmæssig vis.

#	Kontrolaktivitet	Udførte tests	Resultater af tests udført af EY
5.1	Databehandleren skal sikre, at uddatamateriale indeholdende personoplysninger omfattet af Databehandleraftalen kun anvendes af personer, der er beskæftiget med de formål, til hvilke behandlingen af de givne oplysninger foretages, herunder personer, som er beskæftiget med at tilvejebringe uddatamateriale.	Forespurgt til indhold af uddatamateriale, samt hvorledes uddatamateriale behandles. Inspiceret proceduren for beskyttelse af uddatamateriale. Inspiceret, at adgange til uddatamateriale er begrænset til personer med et arbejdsbetinget behov.	Ingen afvigelser konstateret.

#	Kontrolaktivitet	Udførte tests	Resultater af tests udført af EY
5.1a	Uanset udgangspunktet i forrige afsnit må uddatamateriale dog ligeledes anvendes af personer, som er beskæftiget med revision eller drifts- og systemtekniske opgaver i det pågældende system.	Forespurgt til indhold af uddatamateriale, samt hvorledes uddatamateriale behandles. Inspiceret proceduren for beskyttelse af uddatamateriale. Inspiceret liste over brugere med privilegeret adgang til uddata.	Ingen afvigelser konstateret.
5.2	Databehandleren skal opbevare uddatamateriale på en sådan måde, at uvedkommende ikke kan få adgang til at gøre sig bekendt med de oplysninger, som er indeholdt heri.	Inspiceret proceduren for beskyttelse af uddatamateriale. Inspiceret, at adgange til uddatamateriale er begrænset til personer med et arbejdsbetinget behov. Inspiceret dokumentation for adgang til serverrum.	Ingen afvigelser konstateret.
5.3	Databehandleren skal tilintetgøre uddatamateriale, når dette ikke længere skal anvendes i forbindelse med Databehandleraftalen og senest efter en af den Dataansvarlige nærmere fastsat frist. Derudover skal uddatamateriale om enkeltpersoner kunne slettes efter anmodning fra den Dataansvarlige.	Forespurgt til procedure for tilintetgørelse af uddatamateriale.	Vi er blevet informeret om, at kontrollen ikke har været udløst endnu, hvorfor det ikke har været muligt at teste implementeringen. Ingen afvigelser konstateret.
5.4	I forbindelse med tilintetgørelse af uddatamateriale skal Databehandleren træffe passende tekniske og organisatoriske sikkerhedsforanstaltninger mod, at dette uddatamateriale misbruges eller kommer til uvedkommendes kendskab.	Forespurgt til procedure for tilintetgørelse af uddatamateriale.	Vi er blevet informeret om, at kontrollen ikke har været udløst endnu, hvorfor det ikke har været muligt at teste implementeringen. Ingen afvigelser konstateret.

Kontrolmål – Eksterne kommunikationsforbindelser
6. Kontroller giver rimelig grad af sikkerhed for, at eksterne kommunikationsforbindelser er regelmæssigt sikret.

#	Kontrolaktivitet	Udførte tests	Resultater af tests udført af EY
6.1	Databehandleren må kun anvende eksterne kommunikationsforbindelser til behandling af oplysninger omfattet af Databehandleraftalen i forbindelse med aftalens opfyldelse, hvis der træffes særlige foranstaltninger såsom kryptering for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.	Forespurgt til proceduren for ekstern kommunikationsforbindelse og hjemmearbejdspladser. Inspiceret VPN-opsætning med adgang til behandling af oplysninger. Observeret, at det ikke er muligt at tilgå data, uden brug af VPN.	Ingen afvigelser konstateret.

Kontrolmål – Logning
7. Kontroller giver rimelig grad af sikkerhed for, at der foretages logning af personoplysninger, og at disse opbevares forsvarligt.

#	Kontrolaktivitet	Udførte tests	Resultater af tests udført af EY
7.1	Databehandleren skal foretage logning af alle anvendelser af personoplysninger omfattet af Databehandleraftalen.	Inspiceret, at anvendelsen af personoplysninger logges.	Ingen afvigelser konstateret.
7.1a	Logningen, jf. forrige afsnit, skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium.	Inspiceret, at loggen indeholder oplysninger om tidspunkt, bruger, type af anvendelse og det anvendte søgekriterie.	Ingen afvigelser konstateret.
7.1b	Logningen, jf. forrige afsnit, skal opbevares i 6 måneder, medmindre andet er aftalt med den Dataansvarlige, hvorefter den skal slettes.	Inspiceret, at log over brugen af persondata opbevares i6 måneder.	Ingen afvigelser konstateret.

#	Kontrolaktivitet	Udførte tests	Resultater af tests udført af EY
7.2	Databehandleren skal på den Dataansvarliges anmodning uden unødigt ophold udlevere logdata til den Dataansvarlige eller til en tilsynsmyndighed.	Forespurgt til procedure for udlevering af logdata til den Dataansvarlige.	Vi er blevet informeret om, at kontrollen ikke har været udløst endnu, hvorfor det ikke har været muligt at teste implementeringen. Ingen afvigelser konstateret.