Staten og Kommunernes Indkøbsservice

Uafhængig revisors ISAE 3000-erklæring vedrørende procedurer og kontroller etableret til beskyttelse af persondata i indkøbsdatasamarbejdet
pr. 31. maj 2024

Indhold

1 Ledelsens udtalelse

Staten og Kommunernes Indkøbsservice behandler personoplysninger på vegne af de deltagende kommuner i henhold til databehandleraftale.

Medfølgende beskrivelse er udarbejdet til brug for de kunder, der har indkøbsdatasamarbejde hos Staten og Kommunernes Indkøbsservice, 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.

Staten og Kommunernes Indkøbsservice anvender underleverandørerne Deloitte og Right People Group (RPG), som udfører udvikling af modeller, ProAct, som yder backup services, Sentia, som yder hosting services, samt Microsoft, som yder cloud services. Beskrivelsen i sektion 3 medtager kun kontrolmål og kontrolaktiviteter hos SKI og medtager således ikke kontrolmål og underliggende kontrolaktiviteter hos underleverandørerne. Visse kontrolmål kan kun nås, hvis underleverandørernes kontroller, der forudsættes i designet af vores kontroller, er passende designet og operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos kunderne, der forudsættes i designet af Staten og Kommunernes Indkøbsservices kontroller, er passende designet og operationelt effektive sammen med relaterede kontroller hos SKI. Beskrivelsen omfatter ikke kontrolaktiviteter udført af kunderne.

Staten og Kommunernes Indkøbsservice bekræfter, at:

a) Den medfølgende beskrivelse i sektion 3, giver en retvisende beskrivelse af indkøbsdatasamarbejdet, der behandler faktura data pr. 31. maj 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (I) Redegør for, hvordan systemet var designet og implementeret, herunder redegør for:

      i. De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger

      ii. De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger

      iii. De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige

      iv. 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

      v. 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

      vi. De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registrerede

      vii. De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger 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

      viii. Ydelser udført af underleverandører, hvis relevant, herunder om de er medtaget efter helhedsmetoden eller udeladt efter partielmetoden.

      ix. Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kon-

trolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger

(II) de 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 designet pr. 31. maj 2024, hvis relevante kontroller hos underleverandører var operationelt effektive, og kunder har udført de komplementerende kontroller, som forudsættes i designet af Staten og Kommunernes Indkøbsservice's kontroller pr. 31. maj 2024. Kriterierne for denne udtalelse var, at:

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

(II) 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

c) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen.

København, 17. juni 2024

Staten og Kommunernes Indkøbsservice

_____

Jonas Klinting
Økonomidirektør

2 Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til Staten og Kommunernes Indkøbsservice.

Til: Staten og Kommunernes Indkøbsservice og de dataansvarlige

Omfang

Vi har fået som opgave at afgive erklæring om Staten og Kommunernes Indkøbsservices beskrivelse i sektion 3 om indkøbsdatasamarbejdet der behandler faktura data, pr. 31. maj 2024 (beskrivelsen) og om designet af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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

Staten og Kommunernes Indkøbsservice anvender Deloitte, og Right People Group (RPG), som udfører udvikling af modeller, ProAct, som yder backup services, Sentia, som yder hosting services, samt Microsoft, som yder cloud services. Beskrivelsen i sektion 3 medtager kun kontrolmål og relaterede kontroller hos Staten og Kommunernes Indkøbsservice og medtager således ikke kontrolmål og relaterede kontroller hos underleverandørerne. Visse kontrolmål kan kun nås, hvis underleverandørers kontroller, der forudsættes i designet af Staten og Kommunernes Indkøbsservice kontroller, er passende designet og implementeret sammen med de relaterede kontroller hos Staten og Kommunernes Indkøbsservice. Vores handlinger har ikke omfattet kontrolaktiviteter udført af Deloitte, Right People Group, ProAct, Sentia samt Microsoft, og vi har ikke vurderet egnetheden af design eller den implementering af kontrolaktiviteter hos underleverandører.

Staten og Kommunernes Indkøbsservices ansvar

Staten og Kommunernes Indkøbsservice er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i sektion 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter; for at anføre kontrolmålene; identifikation af de risici der påvirker opnåelsen af kontrolmålene; udvælgelsen af de kriterier der er præsenteret i ledelsens udtalelse; samt for designet, implementeringen og operationel effektive kontroller for at nå de anførte kontrolmål.

Vores 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.

EY Godkendt Revisionspartnerselskab 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.

Vores ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Staten og Kommunernes Indkøbsservices beskrivelse samt om design 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 med henblik på at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt designet.

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

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

Som nævnt ovenfor har vi ikke udført handlinger vedrørende den operationelle effektivitet 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.

Begrænsninger i kontroller hos en dataansvarlig

Staten og Kommunernes Indkøbsservices beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved Indkøbssamarbejdet, som hver enkelt dataansvarlig måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden.

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 sektion 1. Det er vores opfattelse,

(a) at beskrivelsen af indkøbsdatasamarbejdet, således som det var designet og implementeret pr. 31. maj 2024, i alle væsentlige henseender er retvisende, og

(b) at kontrollerne, der knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt designet pr. 31. maj 2024, hvis kontroller hos underleverandører og komplementerende kontroller hos dataansvarlige var hensigtsmæssigt designet og implementeret pr. 31. maj 2024.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår af sektion 4.

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt de kommuner, der deltager i indkøbsdatasamarbejdet hos Staten og Kommunernes Indkøbsservice, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

København, 17. juni 2024
EY
Godkendt Revisionspartnerselskab
CVR no.: 30 70 02 28

Jesper Due Sørensen
partner

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 det offentlige indkøb, hvilket bl.a. indebærer at skabe viden om offentligt indkøb. SKI er operatør på indkøbsdatasamarbejdet og forestår indsamlingen og analyserne.

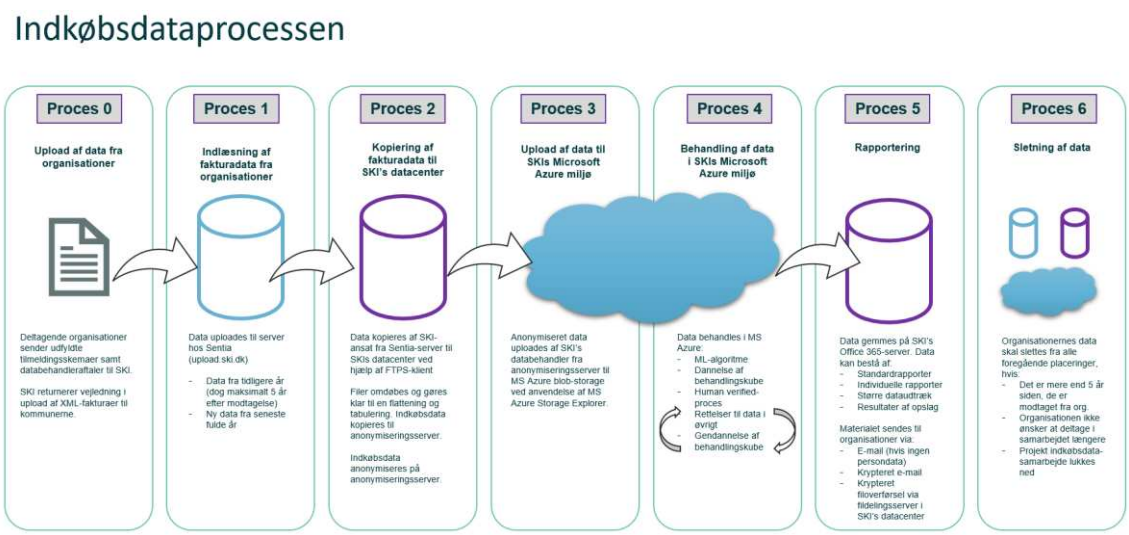
3.3 Beskrivelse af indkøbsdatasamarbejdet

I forbindelse med indkøbsdatasamarbejdet indsamles de deltagende kommuners købsfakturaer for perioden 2014-2022 i årene 2017-2023. I praksis indebærer det, at kommunerne skal overføre en kopi af deres elektroniske fakturadata til indkøbsdatasamarbejdet.

I 2021 hjemtog SKI opgaven med at anonymisere og kategorisere e-fakturaerne – dvs. fjerne personhenførbare data samt tilføje den enkelte fakturalinje en indkøbskategori, såsom "Kuglepenne" eller "Aftørringspapir". Tidligere havde SKI en aftale om løsning af disse opgaver med en it-virksomhed, der fungerede som underleverandør.

Alle SKIs 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 bidrager med deres fakturadata ved at uploade dem til SKI til en sikret, krypteret server, der er hostet hos leverandøren Sentia. SKI gemmer de oprindelige fakturaer, som kommunerne har uploadet, og udbygger denne samling, i takt med at de deltagende kommuner i fremtiden sender nye års

fakturadata til SKI. Dog er det i databehandleraftalen mellem kommunerne og SKI aftalt, at SKI løbende sletter kommunernes elektroniske fakturadata senest 5 år efter modtagelsen af de pågældende data.

Det vil konkret betyde, at fakturadata for perioden 2014-2016, som SKI modtog i foråret 2017, blev slettet i foråret 2022. Fakturadata, som SKI modtog i foråret 2019, vil tilsvarende blive slettet senest i foråret 2024 og så fremdeles.

Den fra kommunerne modtagne fakturadata behandles indledningsvist på en server, der fysisk er placeret på SKIs adresse i Valby. Her udpakkes og tabuleres data. Herefter igangsættes en procedure, der anonymiserer personhenførbare data. Herefter lægges de anonymiserede kommunale data op i "skyen" – i praksis i Microsofts Azure cloud-baserede platform og infrastruktur. Dernæst anvendes machine learning-teknologi i Azure-kuben til at kategorisere hver enkelt af de mange millioner fakturalinjer, så kommunernes samlede indkøb kan sammenlignes på tværs.

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 i praksis databehandler i forhold til hver enkelt kommune, der til gengæld fungerer som dataansvarlig med hensyn til kommunens egne data.

3.6 Beskrivelse af erklæringens omfang

Nærværende erklæring baserer sig alene på kontroller i SKIs eget regi. Dermed er der ikke set på kontrolmål og kontroller hos SKIs backupleverandører ProAct, serverleverandøren Sentia, konsulentvirksomheden Deloitte, samt konsulentvirksomheden Right People Group (ved underdatabehandlerne Nextagenda og dataon), der hjælper med at opbygge og vedligeholde dataløsningen, eller cloud-baserede underleverandører (Microsoft).

Der er ingen fra virksomheden Right People Group (RPG), der har adgang til data. I stedet har RPG engageret to virksomheder, der fungerer som underdatabehandlere – Nextagenda og dataon. Disse to virksomheder er, sammen med Deloitte, i praksis modeludviklere og har adgang til data.

Udvalgte konsulenter fra underdatabehandlerne Deloitte, Nextagenda og dataon har adgange til data på helt tilsvarende vilkår som SKI's egne medarbejdere. Hver enkelt konsulents adgang åbnes og lukkes i takt med, at den pågældende har et arbejdsrelateret behov til at tilgå systemet og den tilknyttede data. De pågældende leverandører har også pligt til at aflevere årlige datasikkerhedserklæringer, som gennemgås af SKI.

3.7 Risikostyring

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

Navn, fødselsdato og CPR-nummer.

Oplysninger om stilling, e-mail, adresse 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 eller oplysninger af privat karakter. Disse behandles alene som led i bortfiltrering hos SKI ved dannelse af analysegrundlaget ud fra fakturaerne.

SKI har etableret en procedure, som har til formål at erstatte personnavne, vejnavne, mailadresser, telefonnumre samt CPR-numre med en generisk beskrivelse. Denne procedure har fjernet langt størstedelen af de personhenførbare data.

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 SKIs side, at kommunerne overholder de udsendte vejledninger om fremsendelse af data. SKI forudsætter desuden, at kommunernes interne procedurer omkring modtagelse og håndtering af fortroligheden vedrørende hentning af data fra SKIs fildelingsserver download.ski.dk 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 SKIs lokation. På lokationen 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 it-udstyr. Yderligere har SKI udarbejdet procedurer, som fastlægger ansvaret for og beskriver behandling af ind- og uddatamateriale, samt sletning af data (1.1b).

SKI har gennemgået Microsofts relevante erklæringer omkring anvendelsen af Microsoft Azure-platformen, og SKI har fundet, at sikkerhedskravene lever op til de krav, som SKI selv er underlagt ifølge den indgåede databehandleraftale med kommunerne (1.2).

I SKIs generelle retningslinjer for informationssikkerhed er der fastlagt retningslinjer for den generelle sikkerhedspolitik i SKI. Disse retningslinjer gennemgås i henhold til årshjulet (1.3).

SKIs generelle retningslinjer for informationssikkerhed indeholder retningslinjer for fjernarbejdspladser, herunder krav om, at adgangen til SKIs systemer sker via krypteret VPN-forbindelse (1.4). SKI har også en række formelle retningslinjer for fjernarbejdspladser (1.4a).

I forbindelse med salg, genbrug og kassation samt reparation af anvendt it-udstyr er der fastlagt procedurer og retningslinjer for informationssikkerhed (1.5) (1.6).

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 indkøbsdatasystemet. Alt inddatamateriale er elektronisk og er placeret på sikrede krypterede servere (2.1).

SKI har i begyndelsen af 2024 slettet produktionsdata (vedrørende året 2018) leveret til samarbejdet, idet de pågældende data ifølge databehandleraftalen skulle slettes. Der er etableret en procedure for sletningen, som har været anvendt (2.2).

Yderligere giver databehandleraftalen den dataansvarlige mulighed for at anmode om at slette ekstraordinært. 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 nyansatte 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 af, 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 SKIs 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.

SKIs it-system registrerer gentagne afviste adgangsforsøg, og adgangen til kontoen spærres automatisk efter 10 forkerte loginforsøg. Herefter skal der gå 15 minutter, før der igen åbnes for nyt loginforsøg. Yderligere fremsendes der en systemgenereret mail til SKIs it-afdeling om spærringen (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 afsnit 3.7 ovenfor) og manuelt ud inden videregivelse. Uddatamateriale indeholdende personoplysninger sendes via en særlig krypteret fildelingsserver download.ski.dk, hvortil en ekstern bruger i den pågældende kommune kan tildeles adgang (5.1). Ud over den begrænsede personkreds har også SKIs interne og eksterne drifts- og systemteknikere samt revision adgang til uddatamateriale indeholdende personoplysninger (5.1a). Uddatamateriale gemmes på krypterede servere på SKIs fysiske adresse, hvor der kræves separat adgangstilladelse (5.2). Der er udarbejdet en procedure omkring sletning af uddatamateriale omhandlende enkeltpersoner eller en enkelt kommunes samlede data (5.3). Ud over ovenstående er SKIs 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. Sådanne fulde datasæt sendes via den krypterede fil-delingsserver, download.ski.dk, til den eller de kontaktperson(er), som kommunen selv har udpeget til samarbejdet.

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 og krypteret fildelingsserver ved uddata med personoplysninger. 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.

Vores test af kontrollers design og implementering har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår af afsnit 3. Eventuelle andre kontrolmål, tilknyttede kontroller og komplementære kontroller hos dataansvarlige, der anvender løsningen, beskrevet i sektion 3, er ikke omfattet af vores test.

Test af design og implementering har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået pr. 31. maj 2024.

4.2 Udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design og implementering 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 designet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller. På de tekniske platforme, databaser og netværkskomponenter har vi testet den specifikke systemopsætning for at påse, om kontroller er designet pr. 31. maj 2024.
Forespørgsler	Forespørgsel af passende personale hos Staten og Kommunernes Indkøbsservice. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.

4.3 Kontrolmål, kontrolaktivitet, test og resultat heraf

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 og adgange til serverrum. Inspiceret, at fratrådte har fået deres adgange fjernet.	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 it-udstyr.	Forespurgt til procedure for sletning af ind- og ud- datamateriale. Inspiceret informationssikkerhedspolitikken. Inspiceret procedurer og instrukser for behandling og destruktion af ind- og uddatamateriale.	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. Inspiceret mødereferat fra informationssikkerhedsrådet.	Ingen afvigelser konstateret.

#	Kontrolaktivitet	Udførte tests	Resultater af tests udført af EY
1.2	Databehandleren skal sikre, at der stilles tilsvarende sikkerhedskrav til underdatabehandleren, som Databehandleren selv er underlagt fra den dataansvarlige. Databehandleren sikrer således, at Microsoft i forbindelse med behandlingen af personoplysninger i Azure-platformen som minimum lever op til samme sikkerhedskrav, som Databehandleren selv er underlagt ("back to back").	Forespurgt til databehandlerens sikring af sikkerhedskravene til underdatabehandlere. Inspiceret, at der er udført egenkontroller i henhold sikkerhedsopsætningen på Azure platformen. Inspiceret, at der indhentes og gennemgås SOC-erklæringer. Inspiceret, at der er foretaget en risikoanalyse af Microsoft som underleverandør.	Ingen afvigelser konstateret.
1.3	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 referat fra seneste møde i informationssikkerhedsrådet. Inspiceret ledelsesgodkendt informationssikkerhedspolitik. Inspiceret årlig gennemgang af interne bestemmelser.	Ingen afvigelser konstateret.
1.4	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, at indkøbsdata ikke kan tilgås uden brug af VPN. Inspiceret udtræk af installeret software, hvor det fremgår, at VPN-klienten er installeret.	Ingen afvigelser konstateret.
1.4a	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, at indkøbsdata ikke kan tilgås uden brug af VPN. Inspiceret udtræk af installeret software, hvor det	Ingen afvigelser konstateret.

#	Kontrolaktivitet	Udførte tests	Resultater af tests udført af EY
		fremgår, at VPN-klienten er installeret.	
1.5	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. Inspiceret mødereferat vedrørende reparation og vedligeholdelse af it-udstyr.	Ingen afvigelser konstateret.
1.6	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. Inspiceret mødereferat vedrørende reparation og vedligeholdelse af it-udstyr.	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.	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.	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 indkøbsdatasamarbejdsprojektet. Inspiceret dokumentation for tildelte adgange til data i indkøbsdatasamarbejdet. Inspiceret procedure samt dokumentation for oprettelse af adgange til indkøbsdatasamarbejdsprojektet.	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.	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 brugeradgang afvises og spærres ved gentagne afviste adgangsforsøg.

#	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 passwordindstillinger. Observeret, at konti lukkes og it underrettes, hvis der benyttes forkert password 10 gange. Forespurgt til rapportering om afviste loginforsøg.	Ingen afvigelser konstateret.

Kontrolmål – Uddatamateriale, som indeholder personoplysninger
5. 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.

#	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. Inspiceret dokumentation for at uddata automatisk slettes som led i dataudvekslingsløsningen.	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. Inspiceret dokumentation for at uddata automatisk slettes som led i dataudvekslingsløsningen.	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 brugen af faktura data logges.

#	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.
7.2	Databehandleren skal på den Dataansvarliges anmodning uden unødigt ophold udlevere logdata til den Dataansvarlige eller til en tilsynsmyndighed.	Inspiceret procedure for udlevering af logdata til den Dataansvarlige. Forespurgt, om der har været anmodninger om udlevering af logdata.	Ingen afvigelser konstateret.

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Jonas Klinting
Økonomidirektør
På vegne af: SKI
Serienummer: 31d78a3a-70aa-400e-9d58-f4a0c86167ad
IP: 62.116.xxx.xxx
2024-06-17 09:00:19 UTC

Jesper Due Sørensen
EY Godkendt Revisionspartnerselskab CVR: 30700228
Partner
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: a6d834d7-442d-428e-ade9-c250dca23ab3
IP: 165.225.xxx.xxx
2024-06-17 09:03:16 UTC

Nils Bonde Christiansen
EY Godkendt Revisionspartnerselskab CVR: 30700228
Statsaut. revisor
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: a4c7bea3-5a9f-4f35-bb2c-9ca1124e41f1
IP: 165.225.xxx.xxx
2024-06-17 09:13:11 UTC