Visma Local Government A/S

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til Visma Local Government A/S' skabelon for databehandleraftale med dataansvarlige

Pr. 27. september 2021

Building a better working world

Indhold

1 Ledelsens udtalelse

Visma Local Government A/S (gældende binavn FirstAgenda A/S og XFlow A/S) behandler personoplysninger på vegne af vores kunder i henhold til indgået databehandleraftaler.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt Visma Local Governments digitale løsninger, dækkende FirstAgenda LetDialog, FirstAgenda Live, FirstAgenda Management, FirstAgenda Prepare og FirstAgenda Publication, EduAdm og XFlow Flex, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som underdatabehandlere og de dataansvarlige selv har udført ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") er overholdt.

Visma Local Government anvender underdatabehandlere til at supportere de digitale løsninger. Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underdatabehandleres kontroller, der forudsættes i designet af vores kontroller, er passende designet og implementeret. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underdatabehandlere.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos dataansvarlige, der forudsættes i designet af dataansvarliges kontroller, er passende designet og fungerer effektivt sammen med relaterede kontroller hos Visma Local Government. Beskrivelsen omfatter ikke kontrolaktiviteter udført af dataansvarlige.

Visma Local Government bekræfter, at:

a) Den medfølgende beskrivelse, sektion 3, giver en retvisende beskrivelse af Visma Local Governments aktiviteter og kontroller i henhold til Visma Local Governments skabelon for databehandleraftaler, i forbindelse med behandling af personoplysninger for dataansvarlige pr. 3. juni 2020:

   (i) Redegør for, hvordan aktiviteter og kontroller var udformet 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 underdatabehandlere, hvis relevant, herunder om de er medtaget efter helhedsmetoden eller udeladt efter partielmetoden.

      ix. Kontroller, som vi har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen.

x. Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger.

(ii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne behandling af personoplysninger under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved behandlingen af personoplysninger, som den enkelte dataansvarlige 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. 27. september 2021, hvis relevante kontroller hos underdatabehandlere fungerer effektivt, og dataansvarlige har udført de komplementerende kontroller, som forudsættes i designet af Visma Local Governments kontroller pr. 27. september 2021. Kriterierne anvendt for at give 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.

Aarhus, den 01. november 2021
Visma Local Government A/S

Kasper Lyhr
adm. direktør

2 Uafhængig revisors erklæring

2.1 Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til Visma Local Governments skabelon for databehandleraftale med dataansvarlige

Til: Visma Local Government og dataansvarlige

2.2 Omfang

Vi har fået som opgave at afgive erklæring om Visma Local Governments beskrivelse af aktiviteter og kontroller i henhold til Visma Local Governments skabelon for databehandleraftaler dækkende FirstAgenda LetDialog, FirstAgenda Live, FirstAgenda Management, FirstAgenda Prepare og FirstAgenda Publication, EduAdm og XFlow Flex, i forbindelse med behandling af personoplysninger for dataansvarlige, og om udformningen og implementeringen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen pr. 27. september 2021.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos de dataansvarlige, der forudsættes i designet af Visma Local Governments kontroller, er passende designet og implementeret sammen med relaterede kontroller hos Visma Local Government. Vores handlinger har ikke omfattet kontrolaktiviteter udført af de dataansvarlige, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos de dataansvarlige.

Visma Local Government anvender underdatabehandlere til at supportere de digitale løsninger. Beskrivelsen i sektion 3 medtager kun kontrolmål og relaterede kontroller hos Visma Local Government og medtager således ikke kontrolmål og relaterede kontroller hos underdatabehandlere.

Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underdatabehandleres kontroller, der forudsættes i designet af Visma Local Governments kontroller, er passende designet og implementeret sammen med de relaterede kontroller hos Visma Local Government. Vores handlinger har ikke omfattet kontrolaktiviteter udført af underdatabehandlere, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos underdatabehandlere.

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

2.3 Visma Local Governments ansvar

Visma Local Government er ansvarlig for udarbejdelsen af beskrivelsen i sektion 3 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 at udforme og implementere kontroller for at opnå de anførte kontrolmål.

2.4 Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i IESBA's Etiske regler, som er baseret på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og 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.

2.5 Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Visma Local Governments beskrivelse samt om udformningen og implementeringen 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 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 udformet og implementeret.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og implementeringen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse i sektion 3, samt for kontrollernes udformning og implementering. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet og implementeret. En erklæringsopgave med sikkerhed af denne type omfatter desuden vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som Visma Local Government har specificeret og beskrevet i sektion 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.

2.6 Begrænsninger i kontroller hos en dataansvarlig

Visma Local Governments beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter, 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.

2.7 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 ledelsens udtalelse. Det er vores opfattelse:

a) at beskrivelsen i afsnit 3, således som denne var udformet og implementeret pr. 27. september 2021, i alle væsentlige henseender er retvisende, og

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 27. september 2021, hvis kontroller hos underdatabehandlere fungerer effektivt, og hvis dataansvarlige har designet og implementeret de komplementerende kontroller, der forudsættes i designet af Visma Local Governments kontroller pr. 27. september 2021.

2.8 Beskrivelse af test af kontroller

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

2.9 Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i sektion 4 er udelukkende tiltænkt dataansvarlige, der har anvendt Visma Local Governments systemer FirstAgenda LetDialog, FirstAgenda Live, FirstAgenda Management, FirstAgenda Prepare og FirstAgenda Publication, EduAdm og XFlow Flex, 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, den 01. november 2021
EY Godkendt Revisionspartnerselskab
CVR-nr. 30 70 02 28

Jesper D. Sørensen
Partner

Per Højmark
statsaut. revisor
mne9230

3 Beskrivelse af ydelse til den dataansvarlige, der forudsætter behandling af personoplysninger

Den dataansvarlige har erhvervet licens til databehandlerens digitale løsninger, hvor den dataansvarlige ved brug af løsningerne indtaster, uploader, importerer eller på anden vis tilføjer data, herunder personoplysninger til løsningerne med henblik på brug.

I forbindelse med leveringen af de digitale løsninger, behandler databehandleren således personoplysninger på vegne af den dataansvarlige efter gældende regler og i overensstemmelse med indgået databehandleraftale. Behandling af personoplysninger sker inden for EU/EØS.

3.1 Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Behandling af den dataansvarliges personoplysninger sker med det formål at opfylde den mellem databehandleren og den dataansvarlige indgåede aftale om databehandlerens levering af de digitale løsninger, som den dataansvarlige har tegnet abonnement på.

3.2 Karakteren af behandlingen

Som ejer og leverandør af løsningerne behandler databehandleren ved generel drift, herunder hosting, visning, organisering, modtagelse, videresendelse, strukturering, tilpasning, implementering, søgning, processering, lagring, gendannelse, sletning, begrænsning, vedligeholdelse, udvikling, logning, support, fejlfinding og andre it-ydelser forbundet med at stille løsningerne til rådighed, de af den dataansvarlige tilføjede personoplysninger.

3.3 Personoplysninger

Typen af personoplysninger, der behandles er:

- Visma Local Government behandler de kategorier af personoplysninger, som den dataansvarlige har instrueret Visma Local Government til og informeret om i databehandleraftalen. Ved brug af løsningerne er der dog mulighed for, at den dataansvarlige kan overlade behandling af al slags data til Visma Local Government henset til den dataansvarliges frie mulighed for at uploade eller på anden vis tilføje løsningen data. Såfremt Visma Local Government får vished om behandling af typer af personoplysninger, der ikke er forudsat i databehandleraftale, vil Visma Local Government underrette den dataansvarlige herom, men det er til enhver tid den dataansvarliges ansvar korrekt at angive de typer af personoplysninger, brugen af løsningerne omfatter. Det fremhæves, at Visma Local Government ikke foretager kontrol hermed, ligesom Visma Local Government ikke kan tilgå den dataansvarliges tilføjede personoplysninger uden særskilt samtykke.

  Kategorier af registrerede personer omfattet af databehandleraftalen:

  - Visma Local Government behandler kun data om de registrerede, som den dataansvarlige har instrueret Visma Local Government til og informeret om i databehandleraftalen. Ved brug af løsningen er der dog mulighed for, at den dataansvarlige kan overlade behandling af personoplysninger om alle personkategorier henset til den dataansvarliges frie mulighed for at uploade eller på anden vis tilføje løsningen data. Såfremt Visma Local Government får vished om behandling af kategori af personer, der ikke er forudsat i databehandleraftale, vil Visma Local Government underrette den dataansvarlige herom, men det er til enhver tid den dataansvarliges ansvar korrekt at angive de kategorier af personer, der er relevante for den dataansvarliges tiltænkte brug af løsningerne. Det fremhæves, at Visma Local Government ikke foretager kontrol hermed, ligesom Visma Local Government ikke kan tilgå den dataansvarliges tilføjede kategorier af registrerede uden særskilt samtykke.

3.4 Praktiske tiltag

Behandling af data udgør kernen af den softwareservice, vi yder til vores kunder. Derfor er vores kunders tiltro og tillid til, at vi kan levere vores service på sikker og fortrolig vis også af helt afgørende betydning for vores forretningsgrundlag. Vi tager derfor databeskyttelse og GDPR meget alvorligt og har et kontinuerligt fokus på at behandle vores kunders data sikkert, herunder ved fortløbende forbedring af vores tekniske og organisatoriske sikkerhedsforanstaltninger.

Følgende er en ikke udtømmende liste over vores sikkerhedsforanstaltninger, som foretages henholdsvis af FirstAgenda og/eller tilkøbt hos leverandører:

Leverandører:

- Brug af anerkendte leverandører, der er certificeret til hosting af de digitale løsninger inden for leverandørens EU/EØS-dataregioner.
- Løbende tjek af softwareløsning og systemer i forhold til OWASP top 10-sårbarheder.
- Brug af redundantmiljøer til sikring af adgang og kontinuerlig drift af softwareløsning.
- Netværksbeskyttelse mod cyber-attacks samt tilkobling til Security Operation Center (SOC) via hosting-leverandør.

Visma Local Government:

- Procedure for brud på persondatasikkerheden.
- Fuld TLS- eller HTTPS-kryptering af data i transit og under opbevaring.
- Højeste standard af anti-malware og antivirus på systemer.
- Brug af "ethical hacker".
- Brug af Multi Factor Authentication-login til softwareløsning og produktionsmiljø.
- Logning af adgang og handlinger i softwareløsningen og systemer.
- Procedurer for tilgang til produktionsmiljø og adgang til kundedata.
- Baggrundstjek af medarbejdere.
- Fysisk sikring af lokaliteter med individuelle adgangsnøglebrikker og koder samt overvågning af faciliteter.

Visma Local Government anvender underdatabehandlere listet nedenfor til at supportere de digitale løsninger. Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underdatabehandleres kontroller, der forudsættes i designet af vores kontroller, er passende designet og implementeret. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underdatabehandlere.

Navn	Beskrivelse af behandling	Digital løsning
Zitcom	Hosting - Denne behandling af data sker i henhold til standard underdatabehandleraftale.	LetDialog, Live, Management, Publication, EduAdm, XFlow
Curanet A/S	Sende SMS'er fra Løsningen - Denne behandling af data sker i henhold til deres standard underdatabehandleraftale.	LetDialog, EduAdm
Fuctional Software, Sentry	Samle fejl og sende advarsler til Databehandleren for at overvåge performance på løsningen. Denne behandling af data sker i	LetDialog, Live, EduAdm

	henhold til deres standard underdatabehandleraftale.	
SendGrid	Service til at sende mail fra Løsningen - Denne behandling af data sker i henhold til deres standard underdatabehandleraftale.	LetDialog, Live, Publication, EduAdm
Zendesk	Håndtering af kundehenvendelser. Denne behandling af data er Zendesk kontraktuelt forpligtet til at foretage indenfor EU/EØS i henhold til deres standard underdatabehandleraftale.	LetDialog, Live, Management, Prepare, Publication, EduAdm, XFlow
Microsoft Azure	Hosting – Denne behandling af data er Azure kontraktuelt forpligtet til at foretage indenfor EU/EØS i henhold til deres standard underdatabehandleraftale.	Live, XFlow
Logz.io	Håndtering af fejllogs - Denne behandling af data sker i henhold til deres standard underdatabehandleraftale.	Management, Publication, XFlow
Binero AB	Binero anvendes til hosting af løsningen, logning af fejlbeskeder ved import af data, herunder lagring og processering af data, og dermed behandles alle data i løsningen, inklusive kundernes personoplysninger. Denne behandling af data sker i henhold til deres standard underdatabehandleraftale.	Prepare
Ubivox ApS	Ubivox anvendes til fremsendelse af e-mails vedrørende produktopdatering og feature releases, og der sker i den forbindelse behandling af brugernes navn og e-mails. Behandlingen foregår i EU/EØS, hvor databehandlerens løsning hostes i henhold til separat underdatabehandleraftale.	Prepare
Amazon Web Services EMEA SARL (AWS)	Hosting - Denne behandling af data er AWS kontraktuelt forpligtet til at foretage inden for dataregion EU-WEST (Irland), og dermed indenfor EU/EØS, i henhold til deres standard underdatabehandleraftale.	XFlow

3.5 Risikovurdering

Visma Local Government har foretaget en kortlægning over risikoen for de registreredes rettigheder, herunder en afvejning af disse risici i forhold til de forholdsregler, der er truffet for at beskytte disse rettigheder.

Selve risikovurderingen består af flere dele, herunder:

- En kortlægning af alle de risici, behandlingen medfører, og en kategorisering (scoring, sandsynlighed og alvorlighed) heraf.
- En vurdering af, hvad der er passende tekniske og organisatoriske foranstaltninger til at sørge for, at forordningen overholdes, og dette kan dokumenteres.

I Visma Local Governments egne risikovurderinger er der ingen høj risiko for de registrerede på tværs af alle typer af registrerede og kategorier af personoplysninger.

3.6 Kontrolforanstaltninger

Visma Local Government har etableret årshjul til systematisk måling og kontrol af behandlingssikkerheden. Konklusioner på kontroller fra årshjul evalueres løbende og mindst en gang i kvartalet af ledelsen. Krævede og vedtagne forbedringer i forlængelse heraf foretages løbende, og underretning herom findes i nyhedsbreve til de dataansvarlige. Visma Local Government har etableret en række foranstaltninger og kontroller for at sikre overholdelse af Databeskyttelsesforordningen og de indgåede databehandleraftaler. De etablerede foranstaltninger og kontroller omfatter følgende kontrolmål:

- Kontrolmål A
  Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale.
- Kontrolmål B
  Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.
- Kontrolmål C
  Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.
- Kontrolmål D
  Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.
- Kontrolmål E
  Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.
- Kontrolmål F
  Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.
- Kontrolmål G
  Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.
- Kontrolmål H
  Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.

- Kontrolmål I
  Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.

Der henvises i øvrigt til afsnit 4, hvor de konkrete kontrolaktiviteter er beskrevet.

3.7 Komplementerende kontroller hos de dataansvarlige

Foruden databehandlerens kontrolforanstaltninger er det den dataansvarliges ansvar at sikre følgende:

Eftersom det udelukkende er den dataansvarlige, der ved brug af løsningen ensidigt indtaster, uploader, importerer eller på anden vis tilføjer data, herunder personoplysninger, til løsningen, skal den dataansvarlige sikre sig, at brugen af løsningen alene sker i henhold til typerne af registrerede og kategorierne af personoplysninger, der er indgået aftale om i den mellem parterne indgåede databehandleraftale.

Ved anmodning om support er det ligeledes den dataansvarliges ansvar at sikre, at der alene gives adgang til eller deles sådanne oplysninger, som løsningen af supporthenvendelsen forudsætter.

Den dataansvarlige skal sikre, at adgange og rettigheder til løsningen er korrekte.

Den dataansvarlige skal sikre sig, at instruksen er lovlig set i forhold til den til enhver tid gældende databeskyttelsesretlig regulering samt sikre sig, at instruksen er hensigtsmæssig set i forhold til den indgåede abonnementsaftale om levering af den digitale løsning og den databehandleraftale, der ligeledes er indgået i den forbindelse.

Løsningen understøtter brug af TLS 1.2-kryptering, men den dataansvarlige er ansvarlig for at sikre installation af behørig upload client for at sikre brug af denne krypteringsstandard og ikke tidligere versioner. Visma Local Government kan bistå hermed.

Ved valg af løsningen er den dataansvarlige bekendt med funktionen for sletning af data. Løsningen understøtter og forudsætter således, at den dataansvarlige selv skal udøve sletning eller tilbagetrækning af data, herunder tilføjet personoplysninger. Den dataansvarlige kan ved anmodning herom lade Visma Local Government forestå dette som nærmere beskrevet i indgået databehandleraftale.

Løsningen understøtter ligeledes den dataansvarliges ansvar ved anmodninger fra registrerede, som den dataansvarlige således selv vil kunne opfylde, dog således at Visma Local Government anerkender sin pligt til at bistå ved anmodninger herom.

4 Test udført af EY

I dette afsnit beskrives de af Visma Local Government definerede kontrolmål og tilknyttede kontroller, som sikrer opnåelse af de enkelte kontrolmål. Herudover beskrives de af EY udførte faktiske test af Visma Local Governments kontroller samt resultaterne af de udførte test.

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 udformning og implementering har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår nedenfor. Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos Visma Local Governments kunder, der anvender løsningen, beskrevet i afsnit 1, er ikke omfattet af vores test.

Vores test af implementering har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev nået pr. 27. september 2021.

4.2 Udførte test

De udførte test 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 designet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Forespørgsler	Forespørgsel af passende personale hos Visma Local Government. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Vi har observeret kontrollernes udførelse.

Kontrolmål A

Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Inspiceret, at procedurer er opdateret.	Ingen afvigelser konstateret.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Inspiceret, at der er etableret procedurer for registrering af henvendelser fra kunderne til sikring af, at behandling af personoplysninger alene foregår i henhold til instruks.	Ingen afvigelser konstateret.
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Inspiceret, at der er procedurer for underretning af den dataansvarlige, i tilfælde hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Forespurgt, om den dataansvarlige er underrettet i tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.	Ingen afvigelser konstateret.

Kontrolmål B

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.1	Der foreligger skriftlige retningslinjer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om retningslinjerne skal opdateres.	Inspiceret, at der er retningslinjer, der sikrer, at der etableres sikkerhedsforanstaltninger i overensstemmelse med skabelon for databehandleraftale. Inspiceret, at retningslinjerne er opdateret.	Ingen afvigelser konstateret.
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed. Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Inspiceret, at databehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Inspiceret, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.	Ingen afvigelser konstateret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirussoftware. Inspiceret, at antivirussoftware er opdateret.	Ingen afvigelser konstateret.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem VPN.	Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en VPN.	Ingen afvigelser konstateret.

Kontrolmål B

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
		Inspiceret tildelt administrativ adgang til at vedligeholde firewall-konfiguration og -regelsæt.	
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Inspiceret opsætningen af VPN, som anvendes til segmentering af netværk for at sikre begrænset adgang til systemer og databaser med personoplysninger.	Ingen afvigelser konstateret.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Forespurgt, om der foreligger procedurer for begrænsning af brugeres adgang til personoplysninger. Forespurgt, om der foreligger formaliserede procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Forespurgt, om de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger. Inspiceret, at brugeres adgange til systemer og databaser er begrænset til medarbejdernes arbejdsbetingede behov.	Ingen afvigelser konstateret.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter:	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysninger, er etableret systemovervågning med alarmering.	Ingen afvigelser konstateret.

Kontrolmål B

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
	► Overvågningsalarmer	Forespurgt, om der er sker opfølgning, samt at forholdet er meddelt de dataansvarlige i behørigt omfang.	
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Forespurgt, om transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af kryptering. Forespurgt, om teknologiske løsninger til kryptering har været tilgængelige og aktiveret. Forespurgt, om firewall kun tillader krypteret datatrafik. Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme.	Vi har konstateret, at der i FirstAgenda Live og FirstAgenda Management blev benyttet TLS 1.0 og TLS 1.1 i stedet for nyere versioner, der sikrer imod MITM (Man-in-the-middle)-angreb. Vi har fået oplyst, at FirstAgenda Live og FirstAgenda Management sidenhen er sikret med TLS 1.2 eller nyere. Ingen afvigelser konstateret.
B.9	Der er etableret logning i systemer, databaser og netværk af følende forhold: ► Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder. ► Sikkerhedshændelser omfattende: - Ændringer i logopsætninger, herunder deaktivering af logning. - Ændringer i systemrettigheder til brugere. - Fejlede forsøg på log-on til systemer, databaser og netværk.	Forespurgt til opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang og opfølgning på logs. Inspiceret eksempel på logning af brugeraktiviteter i operativsystemer, der anvendes til behandling af personoplysninger. Inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod sletning og manipulation.	Ingen afvigelser konstateret.

Kontrolmål B

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
	Logoplysninger er beskyttet mod manipulation og tekniske fejl.		
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, sker altid efter aftale med dataansvarlig. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Forespurgt til procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene varetages i henhold til aftalen.	Ingen afvigelser konstateret.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og/eller penetrationstests.	Forespurgt, om der løbende foretages sårbarhedsscanninger. Inspiceret seneste penetrationstest. Inspiceret, at eventuelle afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret samt meddelt de dataansvarlige i behørigt omfang.	Ingen afvigelser konstateret.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Forespurgt, om de tekniske sikkerhedsparametre og -opsætninger i systemer, databaser og netværk er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.	Ingen afvigelser konstateret.
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Inspiceret, at der foreligger procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger.	Ingen afvigelser konstateret.

Kontrolmål B

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
		Forespurgt, om der foretages regelmæssig vurdering og godkendelse af tildelte brugeradgange.	
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor-autentifikation.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at to-faktor-autentifikation anvendes ved behandling af personoplysninger, der medfører højrisiko for de registrerede. Inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører højrisiko for de registrerede, alene kan ske ved anvendelse af to-faktor-autentifikation.	Ingen afvigelser konstateret.
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler, hvori der opbevares og behandles personoplysninger.	Forespurgt, om det kun er autoriserede personer, der har fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Ingen afvigelser konstateret.

Kontrolmål C

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere. Inspiceret, at proceduren er opdateret.	Ingen afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Inspiceret, at kravene i databehandleraftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Ingen afvigelser konstateret.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: ► Referencer fra tidligere ansættelser ► Straffeattest ► Eksamensbeviser.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Ingen afvigelser konstateret.

Kontrolmål C

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	Forespurgt, om nyansatte medarbejdere har underskrevet en fortrolighedsaftale. Forespurgt, om nyansatte medarbejdere er blevet introduceret til: ► Informationssikkerhedspolitikken ► Procedurer vedrørende databehandling, samt anden relevant information.	Ingen afvigelser konstateret.
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon osv. Inddrages. Inspiceret, at seneste fratrådte medarbejderes rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.	Ingen afvigelser konstateret.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Inspiceret, at ansættelseskontrakten indeholder retningslinjer for, at medarbejdere er underlagt tavshedspligt efter ophørt samarbejde.	Ingen afvigelser konstateret.
C.7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger.	Ingen afvigelser konstateret.

Kontrolmål C

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
		Inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.	

Kontrolmål D

Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
D.2	Krav til databehandlerens opbevaringsperioder og sletterutiner er så vidt muligt implementeret i systemet.	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Forespurgt til, om regler for opbevaringsperioder og sletterutiner er implementeret i systemet.	Ingen afvigelser konstateret.
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige, er data i henhold til aftalen med den dataansvarlige: ► tilbageleveret til den dataansvarlige og/eller ► slettet, hvor det ikke er i modstrid med anden lovgivning.	Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger.	Ingen afvigelser konstateret.

Kontrolmål E

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
E.1	Der er etableret procedurer, som sikrer, at der alene opbevares personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der er krav om løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Forespurgt, om der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Inspiceret, at databehandleraftalerne indeholder information for opbevaring af personoplysninger, samt at dette alene foretages på de lokaliteter, der fremgår af databehandleraftalen, og er godkendt af den dataansvarlige.	Ingen afvigelser konstateret.

Kontrolmål F

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Inspiceret, at underdatabehandlere fra databehandlerens oversigt over underdatabehandlere fremgår af standard databehandleraftalerne.	Ingen afvigelser konstateret.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Forespurgt, om dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlere i erklæringsperioden.	Ingen afvigelser konstateret.
F.4	Databehandleren har pålagt underdatabehandlere de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Inspiceret, at underdatabehandleraftaler indeholder samme krav og forpligtelser, som er anført i standard databehandleraftalerne mellem de dataansvarlige og databehandlere.	Ingen afvigelser konstateret.

Kontrolmål F

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: ► Navn ► CVR-nr. ► Adresse ► Beskrivelse af behandlingen.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen afvigelser konstateret.
F.6	Databehandleren foretager på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Inspiceret seneste dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag o.lign. Inspiceret dokumentation for, at information om opfølgning hos underdatabehandlere meddeles den dataansvarlige, således at denne kan tilrettelægge eventuelt tilsyn.	Ingen afvigelser konstateret.

Kontrolmål G

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at personoplysninger alene overføres til tredjelande eller internationale organisationer i henhold til aftale med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer.	Ingen afvigelser konstateret.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Forespurgt, om der foreligger formaliserede procedurer for sikring af et gyldigt overførselsgrundlag.	Ingen afvigelser konstateret.

Kontrolmål H

Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
H.2	Databehandleren, i det omfang dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Forespurgt, hvorledes databehandleren bistår den dataansvarlige i relation til de registreredes rettigheder.	Ingen afvigelser konstateret.

Kontrolmål I

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
I.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: ► Awareness hos medarbejdere. ► Overvågning af netværkstrafik. ► Opfølgning på logning af tilgang til personoplysninger.	Inspiceret, at databehandler udbyder awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Forespurgt, om netværkstrafik overvåges, samt at der sker opfølgning på anormaliteter, overvågningsalarmer, overførsel af store filer m.v. Forespurgt, om der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang.	Ingen afvigelser konstateret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 48 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Forespurgt underdatabehandlerne, om de har konstateret nogen brud på persondatasikkerheden pr. 27. september 2021. Forespurgt, om databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser. Forespurgt, om registrerede brud på persondatasikkerheden hos databehandleren eller under-	Ingen afvigelser konstateret.

Kontrolmål I

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
		databehandlerne er meddelt de berørte dataansvarlige uden unødig forsinkelse og senest 48 timer efter, at databehandleren er blevet opmærksom på brud på persondatasikkerheden.	
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: ► Karakteren af bruddet på persondatasikkerheden. ► Sandsynlige konsekvenser af bruddet på persondatasikkerheden. ► Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for: ► Beskrivelse af karakteren af bruddet på persondatasikkerheden. ► Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden. ► Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden. Inspiceret dokumentation for, at der ved brud på persondatasikkerheden er truffet foranstaltninger, som har håndteret bruddet på persondatasikkerheden.	Ingen afvigelser konstateret.

Dokumentet er underskrevet med Visma Addo digital signeringsservice.
Underskrifterne i dette dokument er juridisk bindende. Underskrivernes identiteter er registreret og listet herunder.

Med min underskrift bekræfter jeg indholdet i ovenstående dokument.

Kasper Lyhr
Administrerende Direktør

Signer's name supplied by Claus Martin Nielsen
01-11-2021 12:52

Per Højmark

Signer's name supplied by Claus Martin Nielsen
01-11-2021 16:03

Jesper D. Sørensen

Signer's name supplied by Claus Martin Nielsen
01-11-2021 19:13

Visma Addo identifikationsnummer: ec10e21f-aacb-4ab3-8c38-ff5e74b3aae9

Dette dokument er underskrevet digitalt med Visma Addo signeringsservice. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument.

Dokumentet er låst for ændringer og tidsstemplet med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

Sådan kan du verificere, at dokumentet er originalt
Dette dokument er beskyttet med Adobe CDS certifikat. Når du åbner dokumentet i Adobe Reader, kan du se, at dokumentet er certificeret af Visma Addo signeringsservice. Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske signeringsbeviser i dokumentet med Visma Addos validator på denne website https://vismaaddo.net/WebAdmin/#/NemIdValidation

Foruden dette dokument kan ét eller flere dokumenter og bilag være tilknyttet transaktionen.
Alle dokumenter som indgik i transaktionen er listet nedenfor. Hændelsesloggen
beskriver underskrivers hændelser i forbindelse med signering af dokumentet.

Dokumenter i transaktionen

Nærværende dokument
FirstAgenda 2021 - ISAE 3000 databehandleraftale_Type 1_Final.pdf

Ovenstående dokumenter og bilag er fremsendt i underskrevet form til alle partere på e-mail eller som link til download. Underskriver er selv ansvarlig for download og sikker opbevaring af dokumenter og bilag.

Download dokumenter
Har du som underskriver modtaget link til download af dokumenterne vil dette være muligt i op til 10 dage efter underskrift. Herefter vil dokumenterne blive slettet fra Visma Addo.

Hændelseslog for dokument

Hændelseslog for dokumentet

2021-11-01 12:36	Underskriftsprocessen er startet
2021-11-01 12:36	Underskriftsprocessen er startet
2021-11-01 12:36	Underskriftsprocessen er startet
2021-11-01 12:36	En besked er sendt til Kasper Lyhr
2021-11-01 12:36	En besked er sendt til Jesper D. Sørensen
2021-11-01 12:36	En besked er sendt til Per Højmark
2021-11-01 12:37	Dokumentet blev åbnet via linket sendt til Per Højmark
2021-11-01 12:51	Dokumentet blev åbnet via linket sendt til Kasper Lyhr
2021-11-01 12:52	Dokumentet er underskrevet af Kasper Lyhr (IP: 77.241.x.x)
2021-11-01 12:52	Alle dokumenter sendt til Kasper Lyhr er blevet underskrevet
2021-11-01 16:03	Dokumentet er underskrevet af Per Højmark (IP: 145.62.x.x)
2021-11-01 16:03	Alle dokumenter sendt til Per Højmark er blevet underskrevet
2021-11-01 19:12	Dokumentet blev åbnet via linket sendt til Jesper D. Sørensen
2021-11-01 19:13	Dokumentet er underskrevet af Jesper D. Sørensen (IP: 83.72.x.x)
2021-11-01 19:13	Alle dokumenter sendt til Jesper D. Sørensen er blevet underskrevet