

Visma Local Government A/S

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

1. juli 2020 til 30. juni 2021





Indhold

1	Ledelsens udtalelse	2
2	Uafhængig revisors erklæring	4
2.1	Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til FirstAgendas skabelon for databehandleraftale med dataansvarlige	4
2.2	Omfang	4
2.3	FirstAgendas ansvar	4
2.4	Revisors uafhængighed og kvalitetsstyring	4
2.5	Revisors ansvar	4
2.6	Begrænsninger i kontroller hos en dataansvarlig	5
2.7	Konklusion	5
2.8	Beskrivelse af test af kontroller	5
2.9	Tiltænkte brugere og formål	6
3	Beskrivelse af ydelse til den dataansvarlige, der forudsætter behandling af personoplysninger	7
3.1	Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige	7
3.2	Karakteren af behandlingen	7
3.3	Personoplysninger	7
3.4	Praktiske tiltag	7
3.5	Risikovurdering	8
3.6	Kontrolforanstaltninger	8
3.7	Komplementerende kontroller hos de dataansvarlige	9
4	Test udført af EY	10
4.1	Formål og omfang	10
4.2	Udførte test	10
5	Bilag 1	

1 Ledelsens udtalelse

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

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt FirstAgendas mødeeffektiviseringssoftwareløsning, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som underleverandører 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.

FirstAgenda anvender Amazon Web Service EMEA SARL (AWS) til hosting af løsningen, Zendesk Inc. (Zendesk) til behandling af supportanmodninger, og Ubivox ApS anvendes til fremsendelse af e-mails vedrørende produktopdatering og feature releases. Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underleverandørers kontroller, der forudsættes i designet af vores kontroller, er passende designet og fungerer effektivt. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

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 FirstAgenda. Beskrivelsen omfatter ikke kontrolaktiviteter udført af dataansvarlige.

FirstAgenda bekræfter, at:

- a) Den medfølgende beskrivelse, sektion 3, giver en retvisende beskrivelse af FirstAgendas aktiviteter og kontroller i henhold til FirstAgendas skabelon for databehandleraftaler, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen i hele perioden fra 1. juli 2020 til 30. juni 2021. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:
 - (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 underleverandører, 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) Indeholder relevante oplysninger om ændringer til behandling af personoplysninger foretaget i perioden fra 1. juli 2020 til 30. juni 2021.
 - (III) 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 og fungerede effektivt i hele perioden fra 1. juli 2020 til 30. juni 2021, hvis relevante kontroller hos underleverandører fungerer effektivt, og kunder har udført de komplementerende kontroller, som forudsættes i designet af FirstAgendas kontroller i hele perioden fra 1. juli 2020 til 30. juni 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, og
 - (III) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. juli 2020 til 30. juni 2021.
- 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 19. oktober 2021
FirstAgenda 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 FirstAgendas skabelon for databehandleraftale med dataansvarlige

Til: FirstAgenda og dataansvarlige

2.2 Omfang

Vi har fået som opgave at afgive erklæring om FirstAgendas beskrivelse i sektion 3 af aktiviteter og kontroller i henhold til FirstAgendas skabelon for databehandleraftaler, i henhold til databehandleraftale med dataansvarlige, i hele perioden 1. juli 2020 til 30. juni 2021 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos de dataansvarlige, der forudsættes i designet af FirstAgendas kontroller, er passende designet og fungerer effektivt sammen med relaterede kontroller hos FirstAgenda. 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.

FirstAgenda anvender Amazon Web Service EMEA SARL (AWS) til hosting af løsningen, Zendesk Inc. (Zendesk) til behandling af supportanmodninger, og Ubivox ApS anvendes til fremsendelse af e-mails vedrørende produktopdatering og feature releases. Beskrivelsen i sektion 3 medtager kun kontrolmål og relaterede kontroller hos FirstAgenda og medtager således ikke kontrolmål og relaterede kontroller hos AWS, Zendesk og Ubivox. Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underleverandørs kontroller, der forudsættes i designet af FirstAgendas kontroller, er passende designet og fungerer effektivt sammen med de relaterede kontroller hos FirstAgenda. Vores handlinger har ikke omfattet kontrolaktiviteter udført af AWS, Zendesk og Ubivox, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos underleverandører.

2.3 FirstAgendas ansvar

FirstAgenda 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, implementere og effektivt udføre 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 FirstAgendas beskrivelse samt om udformningen og funktionen 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 fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse i sektion 3, samt for kontrollerens udformning og funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i sektion 1.

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

FirstAgendas 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. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

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 i hele perioden fra 1. juli 2020 til 30. juni 2021, i alle væsentlige henseender er retvisende,
- b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. juli 2020 til 30. juni 2021, hvis kontroller hos underleverandører fungerer effektivt, og hvis dataansvarlige har designet og implementeret de komplementerende kontroller, der forudsættes i designet af FirstAgendas kontroller i hele perioden fra 1. juli 2020 til 30. juni 2021, og
- c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået, i alle væsentlige henseender har fungeret effektivt i hele perioden fra 1. juli 2020 til 30. juni 2021, hvis kontroller hos underleverandører fungerer effektivt, og hvis de komplementerende kontroller hos de dataansvarlige, der forudsættes i designet af FirstAgendas kontroller, har fungeret effektivt i hele perioden fra 1. juli 2020 til 30. juni 2021 .

2.8 Beskrivelse af test af kontroller

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



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

2.9 Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i sektion 4 er udelukkende tiltænkt dataansvarlige, der har anvendt FirstAgendas ydelser, 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.

Aarhus, den 19. oktober 2021
EY Godkendt Revisionspartnerselskab
CVR-nr. 30 70 02 28

Jesper Due 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 løsning, hvor den dataansvarlige ved brug af løsningerne indtaster, uploader, importerer eller på anden vis tilføjer data, herunder personoplysninger, til løsningen med henblik på brug.

I forbindelse med leveringen af den digitale løsning behandler databehandleren således personoplysninger på vegne af den dataansvarlige efter gældende regler og i overensstemmelse med indgået databehandleraftale.

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 mødeeffektiviseringssoftwareløsningen, den dataansvarlige har tegnet abonnement på.

3.2 Karakteren af behandlingen

Som ejer og leverandør af softwaren 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 softwareløsningen til rådighed, de af den dataansvarlige tilføjede personoplysninger.

3.3 Personoplysninger

Typen af personoplysninger, der behandles, er:

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

Kategorier af registrerede personer omfattet af databehandleraftalen:

- ▶ FirstAgenda behandler kun data om de registrerede, som den dataansvarlige har instrueret FirstAgenda 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 FirstAgenda får vished om behandling af kategori af personer, der ikke er forudsat i databehandleraftale, vil FirstAgenda 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 løsningen. Det fremhæves, at FirstAgenda ikke foretager kontrol hermed, ligesom FirstAgenda 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 tillid 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.

FirstAgenda:

- ▶ Procedure for behandling af personoplysninger på vegne af den dataansvarlige.
- ▶ Procedure for brud på persondatasikkerheden.
- ▶ Fuld TLS- eller HTTPS-kryptering af data i transit og under opbevaring.
- ▶ Opdateret anti-malware og antivirus på systemer.
- ▶ Brug af Multi Factor Authentication-login til softwareløsning og produktionsmiljø.
- ▶ Logning af adgang og handlinger i løsningerne.
- ▶ Procedure for tilgang til produktionsmiljø og adgang til kundedata.
- ▶ Baggrundstjek af medarbejdere.
- ▶ Fysisk sikring af lokaliteter med individuelle adgangsnøgler og koder samt overvågning af faciliteter.

3.5 Risikovurdering

FirstAgenda 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 FirstAgendas egne risikovurderinger er der ingen høj risiko for de registrerede på tværs af alle typer af registrerede og kategorier af personoplysninger.

3.6 Kontrolforanstaltninger

FirstAgenda 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. FirstAgenda 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 supphørvendelsen forudsætter.

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

Den dataansvarlige skal sikre sig, at instruksen er lovlige set i forhold til den til enhver tid gældende databeskyttelsesretlige 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. FirstAgenda 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 tilføje personoplysninger. Den dataansvarlige kan ved anmodning herom lade FirstAgenda 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 FirstAgenda anerkender sin pligt til at bistå ved anmodninger herom.

4 Test udført af EY

I dette afsnit beskrives de af FirstAgenda definerede kontrolmål og tilknyttede kontroller, som sikrer opnåelse af de enkelte kontrolmål. Herudover beskrives de af EY udførte faktiske test af FirstAgendas 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 FirstAgendas kunder, der anvender løsningen, beskrevet i afsnit 1, er ikke omfattet af vores test.

Vores test af effektivitet har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for de anførte kontrolmål i perioden 1. juli 2020 til 30. juni 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 FirstAgenda. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Vi har observeret kontrollens 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	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks.</p> <p>Der foretages løbende - og mindst en gang årligt - vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.</p> <p>Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen.</p> <p>Inspiceret, at procedurer er opdateret.</p>	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.	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning.</p> <p>Inspiceret, at der er procedurer for underretning af den dataansvarlige, i tilfælde hvor behandling af personoplysninger vurderes at være i strid med lovgivningen.</p> <p>Forespurgt, om den dataansvarlige er underrettet i tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.</p>	<p>FirstAgenda har oplyst, at der ikke har været nogen hændelser i perioden.</p> <p>Ingen afvigelser konstateret.</p>

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	<p>Der foreligger skriftlige retningslinjer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende - og mindst en gang årligt - vurdering af, om retningslinjerne skal opdateres.</p>	<p>Inspiceret, at der er retningslinjer, der sikrer, at der etableres sikkerhedsforanstaltninger i overensstemmelse med skabelon for databehandleraftale.</p> <p>Inspiceret, at retningslinjerne er opdateret.</p>	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.	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed.</p> <p>Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger.</p> <p>Inspiceret, at databehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen.</p> <p>Inspiceret, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.</p>	Ingen afvigelser konstateret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	<p>Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirussoftware.</p> <p>Inspiceret, at antivirussoftware er opdateret.</p>	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.	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	<p>Inspiceret tildelt administrativ adgang til at vedligeholde firewall-konfiguration og -regelsæt.</p> <p>Forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.</p> <p>Inspiceret opsætningen af VPN, som anvendes til segmentering af netværk for at sikre begrænset adgang til systemer og databaser med personoplysninger.</p>	Ingen afvigelser konstateret.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	<p>Inspiceret, at der foreligger procedurer for begrænsning af brugeres adgang til personoplysninger.</p> <p>Inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov.</p> <p>Inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger.</p> <p>Inspiceret, at brugeres adgange til systemer og databaser er begrænset til medarbejdernes arbejdsbetingede behov.</p>	Ingen afvigelser konstateret.
B.7	<p>Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter:</p> <ul style="list-style-type: none"> ▶ Overvågningsalarmer 	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.	Ingen afvigelser konstateret.

Kontrolmål B

Der efterleveres 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.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	<p>Forespurgt, om der er sker opfølgning, samt at forholdet er meddelt de dataansvarlige i behørigt omfang.</p> <p>Inspiceret, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af kryptering.</p> <p>Inspiceret, at teknologiske løsninger til kryptering har været tilgængelige og aktiveret.</p> <p>Inspiceret, at firewall kun tillader krypteret data-traffic.</p> <p>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.</p>	Ingen afvigelser konstateret.
B.9	<p>Der er etableret logning i systemer, databaser og netværk af følgende forhold:</p> <ul style="list-style-type: none"> ▶ Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder. ▶ Sikkerhedshændelser omfattende: <ul style="list-style-type: none"> - Ændringer i logopsætninger, herunder deaktivering af logning. - Ændringer i systemrettigheder til brugere. - Fejlede forsøg på log-on til systemer, databaser og netværk. <p>Logoplysninger er beskyttet mod manipulation og tekniske fejl.</p>	<p>Inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling af personoplysninger, er konfigureret og aktiveret.</p> <p>Inspiceret logning af brugeraktiviteter, der anvendes til behandling af personoplysninger.</p> <p>Inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod sletning og manipulation.</p>	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.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.	Inspiceret procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene varetages i henhold til aftalen. Forespurgt, om udviklings- og testdatabaser, hvor personoplysninger ikke er pseudonymiseret eller anonymiseret, er sket efter aftale med den dataansvarlige og på dennes vegne.	Vi har fået oplyst, at der ikke anvendes produktionsdata til test. Ingen afvigelser konstateret.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og/eller penetrationstest.	Inspiceret, at 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. Inspiceret ved en stikprøve, at 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. Bruges ad-	Inspiceret, at der foreligger procedurer for tildeling og afbrydelse af brugernes adgang til syste-	Ingen afvigelser konstateret.

Kontrolmål B

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

Nr.	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
	gang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	mer og databaser, som anvendes til behandling af personoplysninger. Inspiceret, at 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	<p>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.</p> <p>Der foretages løbende - og mindst en gang årligt - vurdering af, om it-sikkerhedspolitikken skal opdateres.</p>	<p>Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år.</p> <p>Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.</p> <p>Inspiceret, at proceduren er opdateret.</p>	Ingen afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	<p>Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler.</p> <p>Inspiceret, at kravene i databehandleraftalen er dækket af informationssikkerhedspolitikken krav til sikringsforanstaltninger og behandlingssikkerheden.</p>	Ingen afvigelser konstateret.
C.3	<p>Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang:</p> <ul style="list-style-type: none"> ▶ 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.	<p>Inspiceret, at nyansatte medarbejdere har underskrevet en fortrolighedsaftale.</p> <p>Inspiceret, at nyansatte medarbejdere er blevet introduceret til:</p> <ul style="list-style-type: none"> ▶ 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.	<p>Inspiceret procedurer, der sikrer, at fratrådte medarbejders rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon osv. inddrages</p> <p>Inspiceret, at fratrådte medarbejders rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.</p>	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.	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt.</p> <p>Inspiceret, at ansættelseskontrakten indeholder retningslinjer for, at medarbejdere er underlagt tavshedspligt efter ophørt samarbejde.</p>	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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
		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	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende - og mindst en gang årligt - vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	Ingen afvigelser konstateret.
D.2	Krav til databehandlerens opbevaringsperioder og sletterutiner er så vidt muligt implementeret i systemet.	<p>Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.</p> <p>Forespurgt til regler for opbevaringsperioder og sletterutiner implementeret i systemet.</p>	Ingen afvigelser konstateret.
D.3	<p>Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige:</p> <ul style="list-style-type: none"> ▶ tilbageleveret til den dataansvarlige og/eller ▶ slettet, hvor det ikke er i modstrid med anden lovgivning. 	<p>Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger.</p> <p>Inspiceret, at der foreligger dokumentation for ophørte databehandlinger i erklæringsperioden, samt at den aftalte sletning eller tilbagelevering af data er udført.</p>	<p>Der har ikke været ophørte aftaler i perioden.</p> <p>Ingen afvigelser konstateret.</p>

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	<p>Der er etableret procedurer, som sikrer, at der alene opbevares personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der er krav om løbende - og mindst en gang årligt - vurdering af, om procedurerne skal opdateres.</p>	<p>Forespurgt, om der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	Ingen afvigelser konstateret.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	<p>Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder.</p> <p>Inspiceret, at databehandlerskabelonen indeholder information for opbevaring af personoplysninger, samt at dette alene foretages på de lokaliteter, der fremgår af databehandleraftalen, og er godkendt af den dataansvarlige.</p>	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	<p>Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.</p> <p>Der foretages løbende - og mindst en gang årligt - vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	<p>Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere.</p> <p>Inspiceret, at underdatabehandlere fra databehandlerens oversigt over underdatabehandlere fremgår af databehandleraftalerne.</p>	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.	<p>Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere.</p> <p>Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.</p>	Ingen afvigelser konstateret.
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	<p>Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt.</p> <p>Inspiceret, at underdatabehandleraftaler indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.</p>	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: <ul style="list-style-type: none"> ▶ 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 dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelandes overførselsgrundlag og lignende. 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	<p>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.</p> <p>Der foretages løbende - og mindst en gang årligt - vurdering af, om procedurerne skal opdateres.</p>	<p>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.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	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	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder.</p> <p>Der foretages løbende - og mindst en gang årligt - vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	<p>Ingen afvigelser konstateret.</p>
H.2	<p>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.</p>	<p>Inspiceret, at dokumentation for anmodninger om bistand fra den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede er korrekt og rettidigt gennemført.</p>	<p>FirstAgenda har oplyst, at der ikke har været nogen henvendelser i perioden.</p> <p>Ingen afvigelser konstateret.</p>

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	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Der foretages løbende - og mindst en gang årligt - vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Inspiceret, at proceduren er opdateret.</p>	Ingen afvigelser konstateret.
I.2	<p>Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden:</p> <ul style="list-style-type: none"> ▶ Awareness hos medarbejdere. ▶ Overvågning af netværkstrafik. ▶ Opfølgning på logning af tilgang til personoplysninger. 	<p>Inspiceret, at databehandler udbyder awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.</p> <p>Inspiceret dokumentation for, at netværkstrafik overvåges, samt at der sker opfølgning på anomaliteter, overvågningsalarmer, overførsel af store filer m.v.</p> <p>Inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang.</p>	Ingen afvigelser konstateret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødigt forsinkelse og senest 48 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	<p>Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden.</p> <p>Forespurgt underdatabehandlerne, om de har konstateret nogen brud på persondatasikkerheden i erklæringsperioden.</p> <p>Inspiceret, at databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser.</p>	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.4	<p>Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet:</p> <ul style="list-style-type: none"> ▶ Karakteren af bruddet på persondatasikkerheden. ▶ Sandsynlige konsekvenser af bruddet på persondatasikkerheden. ▶ Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. 	<p>Inspiceret, at samtlige registrerede brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødigt forsinkelse og senest 48 timer efter, at databehandleren er blevet opmærksom på brud på persondatasikkerheden.</p> <p>Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for:</p> <ul style="list-style-type: none"> ▶ 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. <p>Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.</p> <p>Inspiceret dokumentation for, at der ved brud på persondatasikkerheden er truffet foranstaltninger, som har håndteret bruddet på persondatasikkerheden.</p>	<p>FirstAgenda har oplyst, at der ikke har været nogen henvendelser i perioden.</p> <p>Ingen afvigelser konstateret.</p>

Standardkontraktbestemmelser

i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på databehandlerens behandling af personoplysninger

mellem

[NAVN]

CVR [CVR-NR]

[ADRESSE]

[POSTNUMMER OG BY]

[LAND]

herefter "den dataansvarlige"

og

Visma Local Government A/S

CVR 37 09 89 22

Søren Frichs Vej 44D,

8230 Åbyhøj

Danmark

herefter "databehandleren"

der hver især er en "part" og sammen udgør "parterne"

HAR AFTALT følgende standardkontraktbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

1. Indhold

2. Præambel	3
3. Den dataansvarliges rettigheder og forpligtelser	3
4. Databehandleren handler efter instruks	4
5. Fortrolighed	4
6. Behandlingssikkerhed	4
7. Anvendelse af underdatabehandlere	5
8. Overførsel til tredjelande eller internationale organisationer	6
9. Bistand til den dataansvarlige	7
10. Underretning om brud på persondatasikkerheden	8
11. Sletning og returnering af oplysninger	8
12. Revision, herunder inspektion	9
13. Parternes aftale om andre forhold	9
14. Ikrafttræden og ophør	9
15. Kontaktpersoner hos den dataansvarlige og databehandleren	10
Bilag A Oplysninger om behandlingen	11
Bilag B Underdatabehandlere	13
Bilag C Instruks vedrørende behandling af personoplysninger	14
Bilag D Parternes regulering af andre forhold	19

2. Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.
2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).
3. I forbindelse med leveringen af databehandlerens digitale løsning **FirstAgenda Prepare**, behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.
4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.
10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes¹ nationale ret og disse Bestemmelser.

¹ Henvvisninger til "medlemsstat" i disse bestemmelser skal forstås som en henvisning til "EØS medlemsstater".

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.
3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

4. Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.
2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5. Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.
2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

- a. Pseudonymisering og kryptering af personoplysninger

- b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
 - c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
 - d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.
2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.
3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).
2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.
3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.
4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-

retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.
6. Databehandleren skal i sin aftale med underdatabehandleren indføre den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.
7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8. Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.
2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.
3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:
 - a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
 - b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland

- c. behandle personoplysningerne i et tredjeland
4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.
5. Disse Bestemmelser skal ikke forveksles med standardkontraktbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

9. Bistand til den dataansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

- a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
 - b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
 - c. indsigtsheden
 - d. retten til berigtigelse
 - e. retten til sletning ("retten til at blive glemt")
 - f. retten til begrænsning af behandling
 - g. underretningsskylten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
 - h. retten til dataportabilitet
 - i. retten til indsigelse
 - j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:
 - a. den dataansvarliges forpligtelse til uden unødigt forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder
 - b. den dataansvarliges forpligtelse til uden unødigt forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis

vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

- c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
 - d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.
3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

10. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.
3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:
 - a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
 - b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
 - c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.
4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet

på vegne af den dataansvarlige og bekræfte over for den dataansvarlig, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

12. Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.
2. Procedurene for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.
3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.
4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.

5. Underskrift

På vegne af den dataansvarlige

Navn [NAVN]
Stilling [STILLING]
Telefonnummer [TELEFONNUMMER]
E-mail [E-MAIL]
Underskrift

På vegne af databehandleren

Navn Kasper Lyhr
Stilling Administrerende direktør
Underskrift

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

For den dataansvarlige

Navn [NAVN]
Stilling [STILLING]
Telefonnummer [TELEFONNUMMER]
E-mail [E-MAIL]

For databehandleren

Navn Søren Skou Jessen
Stilling Compliance Consultant
Telefonnummer +45 29365164
E-mail Dataprivacy@firstagenda.com

Bilag A Oplysninger om behandlingen

A.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Behandlingen af den dataansvarliges personoplysninger sker med det formål at opfylde den indgåede aftale mellem databehandleren og den dataansvarlige om databehandlerens levering af dennes digitale løsning.

A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Som ejer og leverandør af den digitale løsning behandler databehandleren personoplysninger ved sædvanlig 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 databehandlerens levering af den digitale løsning til den dataansvarlige i henhold til aftalen indgået mellem parterne.

A.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Almindelige personoplysninger (jf. Databeskyttelsesforordningens artikel 6)

Navn, e-mailadresse, telefonnummer, og IP-adresse. [DERUDOVER SKAL DATAANSVARLIGE TAGE STILLING TIL OM DER EKSEMPELVIS SKER BEHANDLING AF ANDRE TYPER ALMINDELIGE PERSONOPLSYNINGER] [F.eks. adresse, betalingskortoplysninger, medlemsnummer, type af medlemskab, fremmøde i fitnesscenter og tilmelding til konkrete fitnesshold]

Følsomme personoplysninger (jf. Databeskyttelsesforordningens artikel 9):

- Racemæssig eller etnisk baggrund
- Politisk overbevisning
- Religiøs overbevisning
- Filosofisk overbevisning
- Fagforeningsmæssige tilhørsforhold
- Helbredsforhold herunder misbrug af medicin, narkotika, alkohol m.v.
- Seksuelle forhold

Oplysninger om enkeltpersoners rent private forhold (jf.

Databeskyttelsesforordningens artikel 6, 9, 10, samt databeskyttelseslovens § 8):

- Strafbare forhold
 - Væsentlige sociale problemer
 - Andre rent private forhold, som ikke er nævnt ovenfor:
-
-

Oplysninger om cpr-nummer (jf. databeskyttelseslovens § 11, stk. 1)

- CPR-numre

A.4. Behandlingen omfatter følgende kategorier af registrerede

[BESKRIV KATEGORIERNE AF REGISTREREDE]

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer indtil aftalen mellem parterne om levering af databehandlerens digitale løsning til den dataansvarlige opsiges eller ophæves af parterne.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere.

NAVN	ADRESSE	BESKRIVELSE AF BEHANDLING
Amazon Web Services EMEA SARL (AWS)	38 avenue John F. Kennedy, L-1855 Luxembourg	AWS anvendes til hosting af løsningen, logning af fejlbeskeder ved import af data, herunder lagring og processing af data, og dermed behandles alle data i løsningen, inklusiv kundernes personoplysninger. 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.
Zendesk, Inc. (Zendesk)	1019 Market Street, San Francisco, CA 94103	Zendesk anvendes til behandling af supportanmodninger. Denne behandling af data er Zendesk kontraktuelt forpligtet til at foretage indenfor EU/EØS i henhold til deres standard underdatabehandleraftale.
Ubivox ApS	Østre Stationsvej 43, 3. sal 5000 Odense C	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.

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke foruden den dataansvarliges skriftlige godkendelse gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

Databehandleren skal opretholde en til enhver tid gældende liste over underdatabehandlere på databehandlerens hjemmeside. Underdatabehandleraftalerne rekvireres via hjemmesiden eller ved skriftlig anmodning til databehandleren.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

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 databehandlerens levering af den digitale løsning til den dataansvarlige i henhold til aftalen indgået mellem parterne om levering af databehandlerens digitale løsning.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Databehandlerens digitale løsning omfatter behandling af personoplysninger som følger af nærværende bilag A.

Derfor har databehandleren valgt at implementere et generelt sikkerhedsniveau, at der kan ske behandling heraf.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etableret det nødvendige (og aftalte) sikkerhedsniveau.

Databehandleren skal dog under alle omstændigheder og som minimum gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

Informationssikkerhed

Databehandleren har implementeret politikker, kontroller og processer, som dækker de nedenfor beskrevne informationssikkerhedsområder:

Fortrolighed: Sikre at uautoriserede personer ikke kan få adgang til data, som kan misbruges til skade for databehandlerens kunder, forretningsforbindelser og ansatte.

Integritet: Sikre at systemer indeholder akkurat og komplet information.

Tilgængelighed: Sikre at relevant information og relevante systemer er tilgængelige og stabile.

Instruks

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 en vurdering af, om procedurerne skal opdateres.

Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.

Fysisk sikring og miljøsikring

Databehandleren skal opretholde fysiske sikringsforanstaltninger til sikring af lokaliteter, som anvendes til behandling af personoplysninger herunder opbevaring af personoplysninger omfattet af databehandleraftalen mod uvedkommendes adgang og manipulation.

Databehandleren har passende tekniske foranstaltninger til at begrænse risikoen for enhver uautoriseret adgang til lokaler, hvor der behandles personoplysninger. Databehandleren skal desuden, hvor det er nødvendigt, evaluere og forbedre effektiviteten af sådanne forholdsregler

Databehandleren sikrer, at niveauet for den fysiske sikkerhed til enhver tid er afstemt med det aktuelle trusselbillede samt den følsomhed og mængde af personoplysninger, som databehandleraftalen omfatter.

Kommunikationsforbindelser og kryptering

Databehandleren har passende tekniske foranstaltninger til at beskytte systemer og netværk herunder beskytte data under transmission og adgang via internettet samt til at begrænse risikoen for uautoriseret adgang og/eller installering af skadelig kode.

Databehandleren anvender passende krypteringsteknologier og andre tilsvarende foranstaltninger i overensstemmelse med kravene i lovgivningen, godkendte standarder for kryptering af klassificeret information samt god databehandlingssskik.

I det omfang det er et krav i medfør af gældende national og international lovgivning, standarder vedrørende kryptering af klassificeret information eller god databehandlingssskik anvender databehandler krypteringsteknologier og andre tilsvarende foranstaltninger.

Transmission af personoplysninger over internettet er beskyttet af kryptering. Teknologiske løsninger til kryptering er tilgængelige og aktiveret. Firewall tillader kun krypteret datatrafik. 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.

Firewall eller lignende tekniske foranstaltninger

Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker alene gennem en VPN. Der skal foreligge administrativ adgang til at vedligeholde firewall-konfiguration og -regelsæt.

Antivirus

Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.

Sikkerhedskopiering

Databehandleren skal have interne beredskabsprocedurer, der sikrer genetablering af services uden ugrundet ophold i tilfælde af driftsafbrydelser i henhold til hovedaftalen. Databehandleren sikrer daglig backup.

Sikkerhedskopiering af konfigurationsfiler og data skal finde sted i et ubrudt forløb, således at relevant data kan reetableres. Sikkerhedskopierne opbevares således, at de ikke hændeligt eller ulovligt (eks. ved brand, oversvømmelse, uheld, tyveri eller lignende) tilintetgøres, fortabes, forringes, kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

Sikkerhedskopierne skal opbevares fysisk adskilt fra primære data og i et sikkerhedsgodkendt datacenter.

Anvendelse af hjemme/fjernarbejdspladser

Såfremt der foretages databehandling fra ad hoc og/eller hjemmearbejdspladser, sikre databehandleren at disse lever op til de sikkerhedsmæssige krav i denne databehandleraftale med bilag og lovgivning i øvrigt.

Databehandler skal blandt andet opfylde følgende:

- At der anvendes krypteret forbindelse mellem ad hoc arbejdspladsen og databehandlerens/dataansvarliges netværk

- Databehandlerens har en intern instruks til egne medarbejdere vedrørende ad hoc og hjemmearbejdspladser

Derudover skal databehandleren, hvis det er teknisk muligt, anvende 2-faktor-autentifikation.

Instruktion af medarbejdere

Databehandleren sikrer at ansatte til stadighed er bekendt med og har tilstrækkelig uddannelse og instruktion om databehandlingens formål, politikker og arbejdsgange og om deres tavshedspligt.

Der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt, inden for det seneste år. Informationssikkerhedspolitikken er kommunikeret til relevante interessenter herunder databehandlerens medarbejdere.

Informationssikkerhedspolitikken lever generelt op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler.

Der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.

Medarbejdere har underskrevet en fortrolighedsaftale. Medarbejdere er blevet introduceret til:

- Informationssikkerhedspolitikken
- Procedurer vedrørende databehandling, samt anden relevant information

Der foreligger procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon osv. inddrages.

Der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Ansættelseskontrakten indeholder retningslinjer for, at medarbejdere er underlagt tavshedspligt efter ophørt samarbejde.

Databehandleren udbyder awareness-træning til medarbejderne, der omfatter generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger.

Der foreligger dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.

Bortskaffelse af udstyr

Databehandleren skal have formelle processer med henblik på at sikre, at der sker en effektiv sletning af personoplysninger inden bortskaffelse af elektronisk udstyr.

Logning

1. Der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger.
2. Databehandler sikrer, at sikkerhedsloggens omfang er defineret ud fra en af databehandleren udført risikovurdering.
3. Databehandler sikrer, at der er plads nok til at sikkerhedsloggene kan gemmes for perioden.
4. Databehandler sikrer, at der gennemføres løbende stikprøvekontroller af, at sikkerhedsloggene indeholder det forventede.
5. Databehandler afvejer sikkerhedsloggens slettefrister imellem muligheden for at analysere cyberangreb, understøtte efterforskning og hensynet til beskyttelses af fysiske personers rettigheder og frihedsrettigheder.

6. Databehandler sikrer, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod sletning og manipulation.
7. Databehandler sikrer at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret.
8. Databehandler sikre logning i alle miljøer, hvor personoplysninger behandles.
9. Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder.
10. Ændringer i logopsætninger, herunder deaktivering af logning.
11. Ændringer i systemrettigheder til brugere.
12. Fejlede forsøg på log-on til systemer, databaser og netværk.

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt – inden for nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

Registreredes rettigheder, jf. pkt. 9.1.

- Databehandleren skal bistå med at iagttage de registreredes rettigheder ved bl.a. at kunne give indsigt i, slette, begrænse og berigtige oplysninger samt sørge for at dette også sker hos underdatabehandlerne
- Databehandleren skal bistå med at opfylde de registreredes rettigheder uden unødigt forsinkelse
- Databehandleren skal have udarbejdet en procedure for, hvordan de behandler anmodninger fra en registreret om deres rettigheder

Brud og hændelser, jf. pkt. 9.2.

Informationer som skal sendes:

- Fakta om det konstaterede brud (tid, sted, årsag)
- Hvornår bruddet startede, hvornår det blev opdaget og hvornår bruddet er standset
- Karakteren af bruddet på persondatasikkerheden, herunder om der er sket brud på fortrolighed, integritet og tilgængelighed
- Kategorierne og det omtrentlige antal berørte registrerede hvis dette er muligt
- Kategorierne af personoplysninger hvis dette er muligt
- Navn og kontaktoplysninger til kontaktpunkt hvor yderligere oplysninger kan indhentes
- Beskrivelse af de sandsynlige konsekvenser af bruddet
- Beskrivelse af foranstaltninger der er truffet eller foreslået truffet som led i håndteringen af bruddet og dets mulige skadevirkninger

C.4 Opbevaringsperiode/sletterutine

Personoplysninger opbevares i perioden for parternes aftale om databehandlerens levering af databehandlerens værktøjer og services til den dataansvarlige, eller i henhold til særskilt skriftlig aftale, hvorefter de slettes hos databehandleren.

Ved ophør skal databehandleren således enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse Bestemmelser – har ændret den dataansvarliges oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt herunder elektronisk i tilknytning til Bestemmelserne.

C.5 Lokaltid for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end de, som følger af nærværende databehandleraftale.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler, medmindre en sådan overførsel sker til en af de autoriseret underdatabehandlere nævnt i bilag B. Overførselsgrundlag anvendes i henhold til Databeskyttelsesforordningens Kapitel V om overførsler af personoplysninger til tredjelande eller internationale organisationer. De specifikke overførselsgrundlag følger af gældende bilag B.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

Databehandleren skal inden for en periode af 12 måneder for egen regning indhente en ISAE 3000 revisionserklæring fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret samt disse Bestemmelser.

Revisorerklæringen vil være tilgængelig for den dataansvarlige på databehandlerens hjemmeside.

Den dataansvarlige kan mod betaling anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde anmode om en ny erklæring under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af erklæring er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret samt disse Bestemmelser.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover – mod betaling – adgang til at foretage inspektioner herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt og efter passende forudgående varsling.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv.

C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere

Databehandleren skal årligt for egen regning indhente en revisorerklæring fra en uafhængig tredjepart eller en kontrolrapport vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

Dokumentation for sådanne inspektioner fremsendes ved anmodning herom til den dataansvarlige til orientering.

Bilag D Parternes regulering af andre forhold

Parternes aftale om erstatningsansvar og ansvarsbegrænsning fremgår af aftalen indgået mellem databehandleren og den dataansvarlige om databehandlerens levering af digitale løsninger til den dataansvarlige, så længe denne ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.



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

Med min underskrift bekræfter jeg indholdet i ovenstående dokument.

Jesper Sørensen

Signer's name supplied by Claus Martin Nielsen
19-10-2021 07:00

Kasper Lyhr
Administrerende Direktør

Signer's name supplied by Claus Martin Nielsen
19-10-2021 11:54

Per Højmark

Signer's name supplied by Claus Martin Nielsen
19-10-2021 12:49

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

Dokumentet er låst for ændringer og tidsstempelt 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 signeringservice. 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 - ISAE 3000 databehandleraftale_Type 2 - final.pdf

Ovenstående dokumenter og bilag er fremsendt i underskrevet form til alle parter 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

2021-10-18 16:29 Underskriftsprocessen er startet
2021-10-18 16:29 Underskriftsprocessen er startet
2021-10-18 16:29 Underskriftsprocessen er startet
2021-10-18 16:29 En besked er sendt til Kasper Lyhr
2021-10-18 16:29 En besked er sendt til Jesper Sørensen
2021-10-18 16:29 En besked er sendt til Per Højmark
2021-10-18 16:29 Dokumentet blev åbnet via linket sendt til Kasper Lyhr
2021-10-18 16:31 Dokumentet blev åbnet via linket sendt til Per Højmark
2021-10-19 06:59 Dokumentet blev åbnet via linket sendt til Jesper Sørensen
2021-10-19 07:00 Dokumentet er underskrevet af Jesper Sørensen (IP: 80.62.x.x)
2021-10-19 07:00 Alle dokumenter sendt til Jesper Sørensen er blevet underskrevet
2021-10-19 11:54 Dokumentet er underskrevet af Kasper Lyhr (IP: 77.241.x.x)
2021-10-19 11:54 Alle dokumenter sendt til Kasper Lyhr er blevet underskrevet
2021-10-19 12:49 Dokumentet er underskrevet af Per Højmark (IP: 145.62.x.x)
2021-10-19 12:49 Alle dokumenter sendt til Per Højmark er blevet underskrevet

Visma Addo identifikationsnummer: b56b209f-f21 c-40e9-99e6-4 1f5e79af411

Visma Addo

Visma Consulting • Gærtorvet 1-5 • 1799 Copenhagen V • Denmark
addo@visma.com • www.visma.dk/addo