



# Visma Local Government A/S

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

## Indhold

<b>1</b>	<b>Ledelsens udtalelse</b>	<b>2</b>
<b>2</b>	<b>Uafhængig revisors erklæring</b>	<b>4</b>
2.1	Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til Visma Local Governments skabelon, versionsnummer 1, for databehandleraftale med dataansvarlige.	4
2.2	Omfang	4
2.3	Visma Local Governments ansvar	4
2.4	Revisors uafhængighed og kvalitetsstyring	4
2.5	Vores ansvar	5
2.6	Begrænsninger i kontroller hos en dataansvarlig	5
2.7	Konklusion	5
2.8	Beskrivelse af test af kontroller	6
2.9	Tiltænkte brugere og formål	6
<b>3</b>	<b>Beskrivelse af ydelse til den dataansvarlige, der forudsætter behandling af personoplysninger</b>	<b>7</b>
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	8
3.5	Anvendelse af underdatabehandlere	8
3.6	Risikovurdering	10
3.7	Kontrolforanstaltninger	10
3.8	Komplementerende kontroller hos de dataansvarlige	13
<b>4</b>	<b>Tests udført af EY</b>	<b>14</b>
4.1	Formål og omfang	14
4.2	Udførte tests	14

## 1 Ledelsens udtalelse

Visma Local Government A/S (gældende binavn FirstAgenda A/S, herefter Visma Local Government) behandler personoplysninger på vegne af vores kunder i henhold til indgået Visma Local Governments skabelon for databehandleraftaler, versionsnummer 1, dækkende mødeeffektiviseringssoftwareløsning (FirstAgenda Prepare) og digitale løsninger (LetDialog, FirstAgenda Live, FirstAgenda Management, FirstAgenda Publication, EduAdm, XFlow, FirstAgenda Prepare (Biner) og FirstAgenda Prepare (AWS)).

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt Visma Local Governments mødeeffektiviseringssoftwareløsning (FirstAgenda Prepare) og digitale løsninger (LetDialog, FirstAgenda Live, FirstAgenda Management, FirstAgenda Publication, EduAdm og XFlow, FirstAgenda Prepare (Biner), FirstAgenda Prepare (AWS)), 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.

Visma Local Government anvender underdatabehandlere til support, drift og hosting af de digitale løsninger, som anført i sektion 3.5. Beskrivelsen i sektion 3 medtager kun kontrolmål og kontrolaktiviteter hos Visma Local Government og medtager således ikke kontrolmål og underliggende kontrolaktiviteter hos underdatabehandlere. 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 er operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

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

Visma Local Government bekræfter, at:

- a) Den medfølgende beskrivelse, sektion 3, giver en retvisende beskrivelse af Visma Local Governments aktiviteter og kontroller i henhold til Visma Local Governments skabelon for databehandleraftaler, versionsnummer 1, jf. bilag 1, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen i perioden fra 1. juli 2022 til 30. juni 2023. 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 2022 til 30. juni 2023.
- (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 designet og operationelt effektive i perioden fra 1. juli 2022 til 30. juni 2023, hvis relevante kontroller hos underleverandører var hensigtsmæssigt designet og operationelt effektive, og dataansvarlige har udført de komplementerende kontroller, som forudsættes i designet af Visma Local Governments kontroller i perioden fra 1. juli 2022 til 30. juni 2023. 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 udført konsistent som designet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i perioden fra 1. juli 2022 til 30. juni 2023.
- 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 7. november 2023  
Visma Local Government A/S

Mikkel Bjerregaard  
adm. direktør

## 2 Uafhængig revisors erklæring

### 2.1 Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til Visma Local Governments skabelon, versionsnummer 1, for databehandleraftale med dataansvarlige.

Til: Visma Local Government og dataansvarlige.

### 2.2 Omfang

Vi har fået som opgave at afgive erklæring om Visma Local Governments beskrivelse af aktiviteter og kontroller i henhold til Visma Local Governments skabelon for databehandleraftaler, versionsnummer 1, dækkende mødeeffektiviseringssoftwareløsning (FirstAgenda Prepare) og digitale løsninger (LetDialog, FirstAgenda Live, FirstAgenda Management, FirstAgenda Publication, EduAdm, XFlow, FirstAgenda Prepare (Binero) og FirstAgenda Prepare (AWS)), i henhold til databehandleraftale med dataansvarlige, i perioden 1. juli 2022 til 30. juni 2023 (beskrivelsen) og om designet og den operationelle effektivitet 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 Visma Local Governments kontroller, er passende designet og operationelle effektive sammen med relaterede kontroller hos Visma Local Government. Vores handlinger har ikke omfattet kontrolaktiviteter udført af de dataansvarlige, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos de dataansvarlige.

Visma Local Government anvender underdatabehandlere til at support, drift og hosting af de digitale løsninger, som anført i sektion 3.5. Beskrivelsen i sektion 3 medtager kun kontrolmål og relaterede kontroller hos Visma Local Government og medtager således ikke kontrolmål og relaterede kontroller hos underdatabehandlere. Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underleverandørers kontroller, der forudsættes i designet af Visma Local Governments kontroller, er passende designet og operationel effektive sammen med de relaterede kontroller hos Visma Local Government. Vores handlinger har ikke omfattet kontrolaktiviteter udført af underleverandører, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos underleverandører.

### 2.3 Visma Local Governments ansvar

Visma Local Government er ansvarlig for udarbejdelsen af beskrivelsen i sektion 3 og tilhørende udtalelse i sektion 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene, identifikation af de risici der påvirker opnåelsen af kontrolmålene; udvælgelsen af de kriterier der er præsenteret i ledelsens udtalelse, samt for designet, implementeringen og operationel effektive 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 International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

EY Godkendt Revisionspartnerselskab er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende krav i lov og øvrig regulering.

## 2.5 Vores ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Visma Local Governments beskrivelse samt om designet og operationel effektivitet 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 designet og operationelt effektive.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, designet og operationel effektivitet af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse i sektion 3, samt for kontrollerens design og operationel effektivitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt designet eller ikke er operationelt effektive. Vores handlinger har omfattet test af den operationelle effektivitet af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået.

En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden 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

Visma Local Governments beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved, 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 den operationelle effektivitet 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 designet og implementeret i perioden fra 1. juli 2022 til 30. juni 2023, 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 designet i perioden fra 1. juli 2022 til 30. juni 2023, hvis kontroller hos underleverandører og komplementerende kontroller hos dataansvarlige var hensigtsmæssigt designet og implementeret i perioden fra 1. juli 2022 til 30. juni 2023, som forudsat i designet af Visma Local Governments kontroller, 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 været operationelt effektive i perioden fra 1. juli 2022 til 30. juni 2023, hvis kontroller hos underleverandører var operationelt effektive, og hvis de komplementerende kontroller hos de dataansvarlige, der forudsættes i designet af Visma Local Governments kontroller, har været operationelt effektive i perioden fra 1. juli 2022 til 30. juni 2023.



## Visma Local Government A/S

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

### 2.8 Beskrivelse af test af kontroller

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

### 2.9 Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i sektion 4 er udelukkende tiltænkt dataansvarlige, der har anvendt Visma Local Governments 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.

København, den 7. november 2023  
EY Godkendt Revisionspartner selskab  
CVR-nr. 30 70 02 28

Jesper D. Sørensen  
Partner

Nils B. Christiansen  
statsaut. revisor  
mne34106

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

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

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

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

Formålet med denne beskrivelse er at levere oplysninger til Visma Local Governments kunder og deres interessenter (herunder revisorer) om efterlevelse af indholdet af EU's Generelle Databeskyttelsesforordning ("GDPR").

Desuden er formålet med denne beskrivelse at give oplysninger om behandlingssikkerheden, tekniske og organisatoriske foranstaltninger samt ansvar mellem dataansvarlige (vores kunder) og Visma Local Government A/S.

#### 3.2 **Karakteren af behandlingen**

Som ejer og leverandør af softwareløsningerne behandler Visma Local Government ved generel drift, herunder hosting, visning, organisering, modtagelse, indhentelse, videresendelse, strukturering, tilpasning, implementering, søgning, processering, lagring, gendannelse, sletning, begrænsning, vedligeholdelse, udvikling, modeltræning, logning, support, fejlfinding og andre it-ydelser, de af den dataansvarlige tilføjede personoplysninger, såvel som de personoplysninger den dataansvarlige har muliggjort databehandleren at tilføje softwaren.

#### 3.3 **Personoplysninger**

Typen af personoplysninger, der behandles er:

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

Kategorier af registrerede personer omfattet af databehandleraftalen:

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



### 3.4 Praktiske tiltag

Behandling af data udgør kernen af den service vi yder til vores kunder. Derfor er vores kunders tiltro og tillid til, at vi kan levere vores service på sikker og fortrolig vis også af helt afgørende betydning for vores forretningsgrundlag.

Vi tager derfor databeskyttelse og GDPR meget alvorligt og har et kontinuerligt fokus på at behandle vores kunders data sikkert, herunder ved fortløbende forbedring af vores tekniske og organisatoriske sikkerhedsforanstaltninger.

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

- ▶ it-sikkerhedspolitik
- ▶ Retningslinjer for medarbejdersikkerhed
- ▶ Styring af aktiver, herunder kontrol af udlevering og returnering af aktiver ved ansættelser og fra-trædelser
- ▶ Kryptografi
- ▶ Leverandørforhold og/eller tilsynsplan med underdatabehandler
- ▶ Styring af persondatassikkerhedsbrud og hændeshåndtering
- ▶ Sikre etablering af databehandleraftaler med underdatabehandlere
- ▶ Sikre, at de krav, der pålægges i henhold til lovgivning eller af kunder via kontrakter og databehandleraftaler tilsvarende pålægges underdatabehandlere
- ▶ Kontrol og opdatering af risikovurdering, politikker og procedurer
- ▶ Løbende oplæring af medarbejderne i GDPR
- ▶ Kontrol af adgangsforhold efter arbejdsbetinget behov.

### 3.5 Anvendelse af underdatabehandlere

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.

Når Visma Local Government gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, sikrer Visma Local Government gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, at pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår databehandleraftalen imellem Visma Local Government og den dataansvarlige, 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 databehandleraftalen og databeskyttelsesforordningen. Visma Local Government er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder Visma Local Governments forpligtelser efter indgået databehandleraftalen og databeskyttelsesforordningen.

Underdatabehandleraftale(r) og eventuelle senere ændringer hertil er tilgængelig på hjemmesiderne tilhørende Visma Local Government, hvorved den dataansvarlige 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, gøres ikke tilgængeligt for den dataansvarlige.

Visma Local Government anvender underdatabehandlere listet nedenfor til at supportere de digitale løsninger. Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås,

hvis underdatabehandleres kontroller, der forudsættes i designet af vores kontroller, er passende designet og operationelle effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underdatabehandlere:

Navn	Beskrivelse af behandling	Digital løsning
Binero AB	<p>Binero anvendes til hosting af support-ticket-system.</p> <p>Denne behandling af data sker i henhold til deres standard underdatabehandleraftale.</p> <p>Henvendelse indeholder som udgangspunkt kun et navn og en e-mailadresse. Såfremt selve henvendelsen indeholder personoplysninger, vil der ske behandling heraf.</p>	<ul style="list-style-type: none"> <li>▶ FirstAgenda Prepare (Binero)</li> <li>▶ FirstAgenda Prepare (AWS)</li> <li>▶ XFlow</li> <li>▶ FirstAgenda Management</li> <li>▶ FirstAgenda Live</li> <li>▶ FirstAgenda Publication</li> <li>▶ LetDialog</li> <li>▶ FirstAgenda Prepare</li> <li>▶ EduAdm</li> </ul>
Ubivox ApS	<p>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.</p> <p>Behandlingen foregår i EU/EØS, hvor databehandlerens løsning hostes i henhold til separat underdatabehandleraftale.</p> <p>Ubivox behandler e-mailadresser for at kunne afsende selve e-mailen. Indholdet af selve e-mailen er som udgangspunkt uden personoplysninger.</p>	<ul style="list-style-type: none"> <li>▶ FirstAgenda Prepare (Binero)</li> <li>▶ FirstAgenda Prepare (AWS)</li> <li>▶ FirstAgenda Management</li> <li>▶ FirstAgenda Live</li> <li>▶ FirstAgenda Publication</li> <li>▶ XFlow</li> <li>▶ LetDialog</li> <li>▶ FirstAgenda Prepare</li> <li>▶ EduAdm</li> </ul>
Team.blue Denmark A/S	<p>team.blue anvendes til hosting af SMTP-server til brug for at sende og modtage mails, når databehandleren yder support til den dataansvarlige. Denne behandling af data sker i henhold til deres standard-underdatabehandleraftale.</p>	<ul style="list-style-type: none"> <li>▶ FirstAgenda Prepare (Binero)</li> <li>▶ FirstAgenda Prepare (AWS)</li> <li>▶ FirstAgenda Live</li> <li>▶ FirstAgenda Publication</li> <li>▶ FirstAgenda Management</li> <li>▶ XFlow</li> <li>▶ LetDialog</li> <li>▶ FirstAgenda Prepare</li> <li>▶ EduAdm</li> </ul>
InMobile ApS	<p>InMobile anvendes til at fremsende sms i løsningen. Denne behandling af data sker i henhold til deres standard-underdatabehandleraftale.</p>	<ul style="list-style-type: none"> <li>▶ FirstAgenda Prepare (Binero)</li> <li>▶ FirstAgenda Prepare (AWS)</li> <li>▶ XFlow</li> <li>▶ FirstAgenda Prepare</li> <li>▶ EduAdm</li> </ul>

Navn	Beskrivelse af behandling	Digital løsning
Amazon Web Services EMEA SARL (AWS)	<p>AWS anvendes til hosting af løsningen, logning af fejlbeskeder ved import af data, herunder lagring og processering af data, og dermed behandles alle data i løsningen, inklusiv kundernes personoplysninger.</p> <p>Denne behandling af data er AWS kontraktuelt forpligtet til at foretage inden for dataregion EU-WEST (Irland), og dermed inden for EU/EØS, i henhold til deres standard-underdatabehandleraftale.</p> <p>Eventuel behandling af personoplysninger uden for EU/EØS sker efter EU-Kommissionens standardkontraktbestemmelser (SCC) i henhold til underdatabehandleraftalen.</p>	<ul style="list-style-type: none"> <li>▶ FirstAgenda Prepare (AWS)</li> <li>▶ FirstAgenda Prepare</li> </ul>

### 3.6 Risikovurdering

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

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

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

### 3.7 Kontrolforanstaltninger

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

- ▶ Kontrolmål A  
Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale.
- ▶ Kontrolmål B  
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.
- ▶ Kontrolmål C  
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.
- ▶ Kontrolmål D  
Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.

- ▶ **Kontrolmål E**  
Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.
- ▶ **Kontrolmål F**  
Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.
- ▶ **Kontrolmål G**  
Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.
- ▶ **Kontrolmål H**  
Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.
- ▶ **Kontrolmål I**  
Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.

### **Overførsel af personoplysninger**

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.

Uden dokumenteret instruks fra den dataansvarlige kan Visma Local Government således ikke inden for rammerne af databehandleraftalen:

- 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.

Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, er angivet i databehandleraftalens bilag C, C.6.

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

### **De registreredes rettigheder**

Visma Local Government 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 Visma Local Government så vidt muligt bistår 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) indsigtsretten
- d) retten til berigtigelse
- e) retten til sletning ("retten til at blive glemt")
- f) retten til begrænsning af behandling

- g) underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
- h) retten til dataportabilitet
- i) retten til indsigt
- j) retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering.

#### Håndtering af persondatasikkerhedsbrud

Visma Local Government underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

Underretningen til den dataansvarlige sker om muligt senest 24 timer efter, at Visma Local Government 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.

I overensstemmelse med indgået databehandleraftale bistår Visma Local Government den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at Visma Local Government 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.

I databehandleraftalens bilag C findes nærmere angivet information, som Visma Local Government tilvejebringer i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

#### Fortegnelse

Visma Local Government fører en fortegnelse over alle kategorier af behandlingsaktiviteter, der foretages på vegne af de dataansvarlige. Ledelsen hos Visma Local Government har sikret, at fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige indeholder:

- ▶ Navn og kontaktoplysninger på databehandleren, de dataansvarlige, den dataansvarliges eventuelle repræsentanter og databeskyttelsesrådgivere
- ▶ De kategorier af behandling, der foretages på vegne af den enkelte dataansvarlige
- ▶ Når det er relevant, oplysninger om overførsel til et tredjeland eller en international organisation samt dokumentation for passende garantier
- ▶ Hvis det er muligt, en generel beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger.

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

### 3.8 Komplementerende kontroller hos de dataansvarlige

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

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

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

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

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

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

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

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

## 4 Tests udført af EY

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

### 4.1 Formål og omfang

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

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

Vores test af effektivitet har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål i perioden 1. juli 2022 til 30. juni 2023.

### 4.2 Udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design og operationelle effektivitet er beskrevet nedenfor:

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Forespørgsler	Forespørgsel af passende personale hos Visma Local Government. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.

### Kontrolmål A

Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående 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>Det har ikke været muligt at teste den operationelle effektivitet, fordi der ikke er konstateret tilfælde, hvor en instruks har været i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret.</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.**

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
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.

### 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.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.  Inspiceret tildelt administrativ adgang til at vedligeholde firewall-konfiguration og -regelsæt.	Ingen afvigelser konstateret.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.  Inspiceret opsætningen af VPN, som anvendes til segmentering af netværk for at sikre begrænset adgang til systemer og databaser med personoplysninger.	Ingen afvigelser konstateret.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Inspiceret, at der foreligger procedurer for begrænsning af brugeres adgang til personoplysninger.  Inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov.  Inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger.  Inspiceret, at brugeres adgange til systemer og databaser er begrænset til medarbejdernes arbejdsbetingede behov.	For 4 ud af 8 produkter har det ikke været muligt at få en liste over brugere fra systemet. De 4 produkter vedrører: <ul style="list-style-type: none"> <li>▶ FirstAgenda Live</li> <li>▶ FirstAgenda Management</li> <li>▶ FirstAgenda Publication</li> <li>▶ Letdialog.</li> </ul> Ingen yderligere afvigelser konstateret.

**Kontrolmål B**

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

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
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"> <li>▶ Overvågningsalarmer.</li> </ul>	<p>Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.</p> <p>Inspiceret ved en stikprøve, at der sker opfølgning, samt at forholdet er meddelt til de dataansvarlige i behørigt omfang.</p>	Ingen afvigelser konstateret.
B.8	<p>Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.</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.

### 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.9	<p>Der er etableret logning i systemer, databaser og netværk af følgende forhold:</p> <ul style="list-style-type: none"> <li>▶ Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder.</li> <li>▶ Sikkerhedshændelser omfattende: <ul style="list-style-type: none"> <li>- Ændringer i logopsætninger, herunder deaktivering af logning.</li> <li>- Ændringer i systemrettigheder til brugere.</li> <li>- Fejlede forsøg på log-on til systemer, databaser og netværk.</li> </ul> </li> </ul> <p>Logoplysninger er beskyttet mod manipulation og tekniske fejl.</p>	<p>Inspiceret, at opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang og opfølgning på logs.</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>	<p>Ingen afvigelser konstateret.</p>
B.10	<p>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.</p>	<p>Inspiceret procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene varetages i henhold til aftalen.</p> <p>Forespurgt, om udviklings- og testdatabaser, hvor personoplysninger ikke er pseudonymiseret eller anonymiseret, er sket efter aftale med den dataansvarlige og på dennes vegne.</p>	<p>Det har ikke været muligt at modtage dokumentation for, at data er anonymiseret eller at produktionsdata ikke anvendes til test uden aftale med kunden.</p> <p>Ingen yderligere 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.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og/eller penetrationstests.	Inspiceret, at der løbende foretages sårbarhedsscanninger.  Forespurgt til seneste penetrationstest.  Inspiceret, at eventuelle afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret samt meddelt de dataansvarlige i behørigt omfang.	Der er ikke udført penetrationstest i erklæringsperioden.  Ingen yderligere 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.  Inspiceret ved en stikprøve, at systemer, databaser og netværk er opdateret med aftalte	For 4 ud af 25 stikprøver på ændringer, er der ikke dokumentation på test og godkendelse.  For 5 ud af 5 stikprøver på udvalgte 5 uger på patches, er der ikke dokumentation, der viser, at patches er fuldført i de givne uger.  Ingen yderligere afvigelser konstateret.
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugerens adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Inspiceret, at der foreligger procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger.  Inspiceret, at der foretages regelmæssig vurdering og godkendelse af tildelte brugeradgange.	Det har ikke været muligt at få en fuldstændig liste til understøttelse af den udførte periodiske gennemgang af brugere med adgang til systemerne.  Ingen yderligere afvigelser konstateret.

**Kontrolmål B**

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

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
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 informationssikkerhedspolitikens 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"> <li>▶ Straffeattest.</li> </ul>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.</p> <p>Inspiceret ved en stikprøve for nyansatte medarbejdere i erklæringsperioden, at der er dokumentation for straffeattest.</p>	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 ved en stikprøve, at nyansatte medarbejdere er blevet introduceret til:</p> <ul style="list-style-type: none"> <li>▶ Informationssikkerhedspolitikken.</li> <li>▶ Procedurer vedrørende databehandling, samt anden relevant information.</li> </ul>	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 ved en stikprøve, 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 ved en stikprøve, at fratrædelseserklæring indeholder retningslinjer for, at medarbejdere er underlagt tavshedspligt efter ophørt samarbejde.</p>	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>
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.  Inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.	Ingen afvigelser konstateret.

**Kontrolmål D**

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

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
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>Inspiceret, at der er defineret 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"> <li>▶ Tilbageleveret til den dataansvarlige og/eller</li> <li>▶ Slettet, hvor det ikke er i modstrid med anden lovgivning.</li> </ul>	<p>Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger.</p> <p>Inspiceret ved en stikprøve for ophørte databehandlinger i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.</p>	Ingen afvigelser konstateret.

**Kontrolmål E**

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

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
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>Inspiceret, at der foreligger formaliserede procedurer for, at 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, 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	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.  Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.  Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere.  Inspiceret ved en stikprøve, at underdatabehandlere fra databehandlerens oversigt over underdatabehandlere fremgår af databehandleraftalerne.	Ingen afvigelser konstateret.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere.  Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	Ingen afvigelser konstateret.
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt.  Inspiceret ved en stikprøve, at underdatabehandleraftaler indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	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	<p>Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af:</p> <ul style="list-style-type: none"> <li>▶ Navn</li> <li>▶ CVR-nr.</li> <li>▶ Adresse</li> <li>▶ Beskrivelse af behandlingen.</li> </ul>	<p>Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere.</p> <p>Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.</p>	Ingen afvigelser konstateret.
F.6	<p>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.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne.</p> <p>Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne.</p> <p>Inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende.</p> <p>Inspiceret dokumentation for, at information om opfølgning hos underdatabehandlere meddeles den dataansvarlige, således at denne kan tilrettelægge eventuelt tilsyn.</p>	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.	<p>Forespurgt, om der foreligger formaliserede procedurer for sikring af et gyldigt overførselsgrundlag.</p> <p>Inspiceret, at anvendte underleverandør grundlagt i USA er godkendte virksomheder af EU, og inkluderer i den offentligt godkendte liste af serviceleverandører i USA.</p>	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>Forespurgt om der har været 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>Det har ikke været muligt at teste den operationelle effektivitet, da der ikke har været anmodninger i erklæringsperioden.</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"> <li>▶ Awareness hos medarbejdere.</li> <li>▶ Overvågning af netværkstrafik.</li> <li>▶ Opfølgning på logning af tilgang til personoplysninger.</li> </ul>	<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 24 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 registrerede brud på persondatasikkerheden.</p> <p>Inspiceret, at registrerede brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødigt forsinkelse og senest 24 timer efter, at databehandleren er blevet opmærksom på brud på persondatasikkerheden.</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"> <li>▶ Karakteren af bruddet på persondatasikkerheden.</li> <li>▶ Sandsynlige konsekvenser af bruddet på persondatasikkerheden.</li> <li>▶ Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.</li> </ul>	<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"> <li>▶ Beskrivelse af karakteren af bruddet på persondatasikkerheden.</li> <li>▶ Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden.</li> <li>▶ Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.</li> </ul> <p>Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.</p> <p>Forespurgt om der har været dokumentation for, at der ved brud på persondatasikkerheden er truffet foranstaltninger, som har håndteret bruddet på persondatasikkerheden.</p>	<p>Det har ikke været muligt at teste den operationelle effektivitet, da der ikke har været anmodninger i erklæringsperioden.</p> <p>Ingen afvigelser konstateret.</p>

# PENNEO

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

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

## Mikkel Bjerregaard

### Managing Director

På vegne af: Visma Local Government A/S

Serienummer: 1aa56558-46d4-4572-a074-5ffd629ad3af

IP: 87.63.xxx.xxx

2023-11-07 11:44:30 UTC



## Nils Bonde Christiansen

EY Godkendt Revisionspartnerselskab CVR: 30700228

### Statsautoriseret revisor

På vegne af: EY Godkendt Revisionspartnerselskab

Serienummer: a4c7bea3-5a9f-4f35-bb2c-9ca1124e41f1

IP: 82.99.xxx.xxx

2023-11-07 11:51:46 UTC



## Jesper Due Sørensen

EY Godkendt Revisionspartnerselskab CVR: 30700228

### Partner

På vegne af: EY Godkendt Revisionspartnerselskab

Serienummer: a6d834d7-442d-428e-ade9-c250dca23ab3

IP: 83.73.xxx.xxx

2023-11-07 12:44:21 UTC



Penneo dokumentnøgle: 4AW22-YY0PZ-U6U3X-O4JSN-CKK31-A1DMJ

Dette dokument er underskrevet digitalt via **Penneo.com**. 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 sikre, at dokumentet er originalt

Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet

i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service <penneo@penneo.com>**. Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske signeringsbeviser indlejret i dokumentet ved at anvende Penneos validator på følgende websted: **<https://penneo.com/validator>**