Visma Plandisc A/S

Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger pr. 22. februar 2024 i henhold til databehandleraftaler med dataansvarlige

Februar 2024

Indholdsfortegnelse

1. Ledelsens udtalelse 3
2. Uafhængig revisors erklæring 5
3. Beskrivelse af behandling 8
4. Kontrolmål, kontrolaktivitet, test og resultat heraf 14

1 Ledelsens udtalelse

Visma Plandisc A/S behandler personoplysninger på vegne af dataansvarlige i henhold til databehandleraftaler.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt Visma Plandisc A/S' digitale løsninger, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som den 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" og "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesreglerne") er overholdt.

Visma Plandisc A/S anvender Microsoft, Ipregistry, Safespring AWS, Webhostingog Visma som underdatabehandlere. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som underdatabehandlerne varetager for Visma Plandisc A/S.

Enkelte af de kontrolmål, der er anført i vores beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos de dataansvarlige er hensigtsmæssigt udformet sammen med vores kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen af disse komplementære kontroller.

Visma Plandisc A/S bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en tilfredsstillende præsentation af Visma Plandisc A/S' digitale løsninger, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesreglerne pr. 22. februar 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan Visma Plandisc A/S' digitale løsninger var udformet og implementeret, herunder redegør for:

   - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
   - De processer i både it-systemer og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger
   - De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige
   - 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
   - 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
   - De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underretning af de registrerede
   - De processer, der sikrer passende tekniske og organisatoriske sikkerhedsforanstaltninger 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

- Kontroller, som vi med henvisning til afgrænsningen af Visma Plandisc A/S' digitale løsninger har forudsat ville være implementeret af den dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen

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

(ii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af Visma Plandisc A/S' digitale løsninger til behandling af personoplysninger til 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 Visma Plandisc A/S' digitale løsninger, som den enkelte dataansvarlige måtte anse vigtigt efter sine særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. 22. februar 2024. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

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

Aarhus, den 28. februar 2024
Visma Plandisc A/S

Torben Stigaard
Partner, Managing Director

2 Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger pr. 22. februar 2024 i henhold til databehandleraftaler med dataansvarlige

Til: Visma Plandisc A/S og dataansvarlige

Omfang

Vi har fået som opgave at afgive erklæring om Visma Plandisc A/S' beskrivelse i afsnit 3 af Visma Plandisc A/S' digitale løsninger i henhold til databehandleraftaler med dataansvarlige pr. 22. februar 2024 (beskrivelsen) og om udformningen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Nærværende erklæring omfatter, om Visma Plandisc A/S har udformet hensigtsmæssige kontroller, der knytter sig til de kontrolmål, der fremgår af afsnit 4. Erklæringen omfatter ikke en vurdering af Visma Plandisc A/S' generelle efterlevelse af kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" og "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesreglerne").

Visma Plandisc A/S anvender Microsoft, Ipregistry, Safespring AWS, Webhostingog Visma som underdatabehandlere. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som underdatabehandlere varetager for Visma Plandisc A/S.

Enkelte af de kontrolmål, der er anført Visma Plandisc A/S' beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos de dataansvarlige er hensigtsmæssigt udformet sammen med Visma Plandisc A/S' kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen af disse komplementære kontroller.

Vi har ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i afsnit 4, og udtrykker derfor ingen konklusion herom.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Visma Plandisc A/S' ansvar

Visma Plandisc A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for at udforme kontroller for at opnå de anførte kontrolmål.

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.

Vores revisionsfirma anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Visma Plandisc A/S' beskrivelse samt om udformningen af de kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 (ajourført), "Andre erklæringer med sikkerhed end revision eller review af historiske finansielle oplysninger", og de yderligere krav, der er gældende i Danmark, med henblik på at opnå høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er tilfredsstillende præsenteret, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af sine digitale løsninger samt for kontrollernes udformning. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er tilfredsstillende præsenteret, og at kontrollerne ikke er hensigtsmæssigt udformet. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som databehandleren har specificeret og beskrevet i ledelsens udtalelse.

Som nævnt ovenfor har vi ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i afsnit 4, og udtrykker derfor ingen konklusion herom.

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

Begrænsninger i kontroller hos en databehandler

Visma Plandisc A/S' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved Visma Plandisc A/S' digitale løsninger, som hver enkelt dataansvarlig måtte anse for vigtige efter sine særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i ledelsens udtalelse. Det er vores opfattelse,

a) at beskrivelsen af Visma Plandisc A/S' digitale løsninger, således som de var udformet og implementeret pr. 22. februar 2024, i alle væsentlige henseender er tilfredsstillende præsenteret, og

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 22. februar 2024.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultaterne af disse test fremgår af afsnit 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt dataansvarlige, der har anvendt Visma Plandisc A/S' digitale løsninger, og 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 databeskyttelsesreglerne er overholdt.

Aarhus, den 28. februar 2024
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 77 12 31

Jesper Parsberg Madsen
statsautoriseret revisor
mne26801

3 Beskrivelse af behandling

Formålet med denne beskrivelse er at levere oplysninger til Visma Plandisc A/S' 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 Plandisc A/S.

3.1 Karakteren af behandlingen

Den dataansvarlige har erhvervet licens til Visma Plandisc A/S' 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 løsningerne behandler databehandleren således personoplysninger på vegne af den dataansvarlige efter gældende regler og i overensstemmelse med indgået databehandleraftale.

3.2 Personoplysninger

Typen af personoplysninger, der behandles, er almindelige personoplysninger såsom:

1. Navn
2. Telefonnummer
3. E-mailadresse
4. IP-adresse.

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

Kategorier af registrerede personer omfattet af databehandleraftalen:

1. Den dataansvarliges kunder.

Visma Plandisc A/S behandler kun data om de registrerede, som den dataansvarlige har instrueret Visma Plandisc A/S i 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 data i løsningen. Såfremt Visma Plandisc A/S får vished om behandling af kategori af personer, der ikke er forudsat i databehandleraftalen, vil Visma Plandisc A/S 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 Plandisc A/S ikke foretager kontrol hermed, ligesom Visma Plandisc A/S ikke kan tilgå den dataansvarliges tilføjede kategorier af registrerede uden særskilt samtykke.

3.3 Instruks fra den dataansvarlige

1. Visma Plandisc A/S 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 fremgår af den indgåede databehandleraftale og er nærmere specificeret i gældende bilag A og C.

2. Visma Plandisc A/S underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

3. Visma Plandisc A/S har sikret, at der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. Visma Plandisc A/S udfører alene den behandling af personoplysninger, som fremgår af instruks fra den dataansvarlige.

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 Plandisc A/S og/eller er tilkøbt hos leverandører:

- It-sikkerhedspolitik
- Retningslinjer for medarbejdersikkerhed
- Styring af aktiver, herunder kontrol af udlevering og returnering af aktiver ved ansættelser og fratrædelser
- Kryptografi
- Leverandørforhold og/eller tilsynsplan med underdatabehandler
- Styring af persondatassikkerhedsbrud og hændelseshåndtering
- Sikring af etablering af databehandleraftaler med underdatabehandlere
- Sikring af, 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 Plandisc A/S gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, sikrer Visma Plandisc A/S gennem en kontrakt eller et andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret at pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af databehandleraftalen i mellem Visma Plandisc A/S 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 Plandisc A/S er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder Visma Plandisc A/S' forpligtelser efter indgået databehandleraftalen og databeskyttelsesforordningen.

Underdatabehandleraftale(r) og eventuelle senere ændringer hertil er tilgængelig ved henvendelse til Visma Plandisc A/S og/eller på hjemmesiderne tilhørende Visma Plandisc A/S, 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 tilgængelige for den dataansvarlige.

3.6 Risikovurdering

Visma Plandisc A/S 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 at dette kan dokumenteres.

I Visma Plandisc A/S' 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 Plandisc A/S har etableret et årshjul til systematisk måling og kontrol af behandlingssikkerheden. Konklusioner på kontroller fra årshjulet 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 Plandisc A/S 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.

3.8 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 Plandisc A/S 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.

3.9 De registreredes rettigheder

Visma Plandisc A/S 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 Plandisc A/S 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 indsigelse

j) retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering.

3.10 Håndtering af persondatasikkerhedsbrud

Visma Plandisc A/S underretter uden unødig 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 Plandisc A/S 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 den indgåede databehandleraftale bistår Visma Plandisc A/S den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at Visma Plandisc A/S 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 Plandisc A/S tilvejebringer i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

3.11 Fortegnelse

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

- navn og kontaktoplysninger på databehandleren, de dataansvarlige og 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.

3.12 Komplementære 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 personoplysninger er ajourførte.

- Den dataansvarlige skal sikre, at den fornødne hjemmel til behandlingen er til stede.

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

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

4 Kontrolmål, kontrolaktivitet, test og resultat heraf

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	PwC's udførte test	Resultat af test
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser noteret.
A.2	Databehandleren udfører alene den behandling af personoplysninger, som fremgår af instruks fra den dataansvarlige.	Inspiceret, at ledelsen sikrer, at behandlingen af personoplysninger alene foregår i henhold til instruks. Inspiceret ved en stikprøve på en enkelt behandling af personoplysninger, at denne foregår i overensstemmelse med instruks.	Ingen afvigelser noteret.
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Inspiceret, at der er procedurer for underretning af den dataansvarlige, i tilfælde hvor behandling af personoplysninger vurderes at være i strid med lovgivningen.	Ingen afvigelser noteret.

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikkerhedsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Inspiceret, at procedurerne er opdateret. Inspiceret ved en stikprøve på en enkelt databehandleraftale, at der er etableret de aftalte sikkerhedsforanstaltninger.	Ingen afvigelser noteret.
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 sikkerhedsforanstaltninger, der er aftalt med den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandleren foretager en risikovurdering for at opnå en passende sikkerhed. Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Inspiceret, at databehandleren har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Inspiceret, at databehandleren har implementeret de sikkerhedsforanstaltninger, der er aftalt med den dataansvarlige.	Ingen afvigelser noteret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirussoftware. Inspiceret, at antivirussoftware er opdateret.	Ingen afvigelser noteret.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Inspiceret, at firewallen er konfigureret i henhold til den interne politik herfor.	Ingen afvigelser noteret.

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
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 netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering.	Ingen afvigelser noteret.
B.6	Adgang til personoplysninger er isoleret til brugere med et arbejdsbetinget behov herfor.	Inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugernes 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 ved en stikprøve på en enkelt brugers adgange til systemer og databaser, at disse er begrænset til medarbejdernes arbejdsbetingede behov.	Ingen afvigelser noteret.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering, eksempelvis i tilfælde af kompromittering.	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.	Ingen afvigelser noteret.

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail. TLS-kryptering i forbindelse med transmission af e-mails overholder Datatilsynets krav på området.	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. Inspiceret, at teknologiske løsninger til kryptering er tilgængelige og aktiveret. Inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail.	Ingen afvigelser noteret.
B.9	Der er etableret logning i systemer, databaser og netværk af følgende forhold: • Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder • Sikkerhedshændelser omfattende: ○ Ændringer i logopsætninger, herunder deaktivering af logning ○ Ændringer i systemrettigheder til brugere ○ Fejlede forsøg på log-on til systemer, databaser og netværk. Logoplysningerne er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang af og opfølgning på logge. Inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret. Inspiceret, at opsamlede oplysninger om brugeraktivitet i logge er beskyttet mod manipulation og sletning. Inspiceret ved en stikprøve på en enkelt dags logning, at logfilerne har det forventede indhold i forhold til opsætning, og at der er dokumentation for den foretagne opfølgning og håndtering af eventuelle sikkerhedshændelser. Inspiceret ved en stikprøve på en enkelt dags logning, at der er dokumentation for den foretagne opfølgning på aktiviteter udført af systemadministratorer og andre med særlige rettigheder.	Ingen afvigelser noteret.

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form. Inspiceret ved en stikprøve på en enkelt udviklings- og testdatabase, at personoplysningerne heri er pseudonymiseret eller anonymiseret. Inspiceret ved en stikprøve på en enkelt udviklings- og testdatabase, hvor personoplysningerne ikke er pseudonymiseret eller anonymiseret, at dette er sket efter aftale med den dataansvarlige og på dennes vegne.	Ingen afvigelser noteret.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests. Væsentlige sårbarheder udbedres inden for en fastsat og acceptabel tidshorisont.	Inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførelse af sårbarhedsscanninger og penetrationstests. Inspiceret ved en enkelt stikprøve, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger.	Ingen afvigelser noteret.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches. Sikkerhedspatches installeres jf. leverandørens anbefalinger og udgivelsescyklus.	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 udtræk af tekniske sikkerhedsparametre og -opsætninger, at systemer, databaser og netværk er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.	Ingen afvigelser noteret.

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
B.13	Der er en formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugernes adgang revurderes regelmæssigt og minimum hver sjette måned, herunder revurderes, om rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Inspiceret ved en stikprøve på en enkelt medarbejders adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov. Inspiceret ved en stikprøve på en enkelt fratrådt medarbejder, at dennes adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Inspiceret, at der foreligger dokumentation for en regelmæssig – mindst årlig – vurdering og godkendelse af tildelte brugeradgange.	Ingen afvigelser noteret.
B.14	Privilegeret adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører høj risiko for de registrerede, sker som minimum ved anvendelse af tofaktorautentifikation eller via en sikret jumphost-løsning.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at tofaktorautentifikation anvendes ved behandling af personoplysninger, der medfører høj risiko for de registrerede. Inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører høj risiko for de registrerede, alene kan ske ved anvendelse af tofaktorautentifikation.	Ingen afvigelser noteret.
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Inspiceret dokumentation for, at kun autoriserede personer har fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Ingen afvigelser noteret.

Kontrolmål C:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. Informationssikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst én gang årligt – vurdering af, om informationssikkerhedspolitikken skal opdateres.	Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Ingen afvigelser noteret.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikkerhedsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Inspiceret ved en stikprøve på en enkelt databehandleraftale, at kravene i aftalen er dækket af informationssikkerhedspolitikkens krav til sikkerhedsforanstaltninger og behandlingssikkerheden.	Ingen afvigelser noteret.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbeviser.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Inspiceret ved en stikprøve på en enkelt databehandleraftale, at kravene til efterprøvning af medarbejdere i aftalen er dækket af databehandlerens procedurer for efterprøvning. Inspiceret ved en stikprøve på en enkelt nyansat medarbejder, at der er dokumentation for, at efterprøvningen har omfattet: • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbeviser.	Ingen afvigelser noteret.

Kontrolmål C:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
C.4	Ved ansættelse underskriver medarbejderne en fortrolighedsaftale. Endvidere bliver medarbejderne introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejdernes behandling af personoplysninger.	Inspiceret ved en stikprøve på en enkelte nyansat medarbejder, at den pågældende medarbejder har underskrevet en fortrolighedsaftale. Inspiceret ved en stikprøve på en enkelt nyansat medarbejder, at den pågældende medarbejder er blevet introduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling samt anden relevant information.	Ingen afvigelser noteret.
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelsen, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages. Inspiceret ved en stikprøve på en enkelt fratrådt medarbejder , at rettighederne er inaktiveret eller ophørt, samt at aktiverne er inddraget.	Ingen afvigelser noteret.
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, som databehandleren udfører for de dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Inspiceret ved en stikprøve på en enkelt fratrådt medarbejder, at der er dokumentation for opretholdelse af fortrolighedsaftalen og generel tavshedspligt.	Ingen afvigelser noteret.

Kontrolmål C:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
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 noteret.

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	PwC's udførte test	Resultat af test
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser noteret.
D.2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: • Ved afslutningen af abonnement sletter Plandisc data efter 90 dage.	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Inspiceret ved en stikprøve på en enkelt databehandling fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder. Inspiceret ved en stikprøve på en enkelt databehandling fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysningerne er slettet i overensstemmelse med de aftalte sletterutiner.	Ingen afvigelser noteret.
D.3	Ved ophør af behandlingen af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Inspiceret, at der foreligger formaliserede procedurer for behandlingen af den dataansvarliges data ved ophør af behandlingen af personoplysninger. Inspiceret ved en stikprøve på en enkelt ophørt databehandling, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	Ingen afvigelser noteret.

Kontrolmål E:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Inspiceret, at procedurerne er opdateret. Inspiceret ved en stikprøve på en enkelt databehandling fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Ingen afvigelser noteret.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Inspiceret ved en stikprøve på en enkelt databehandling fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser noteret.

Kontrolmål F:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af 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 én 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 noteret.
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 på en enkelt underdatabehandler fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser noteret.
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 anvendelsen af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelsen af underdatabehandlere.	Ingen afvigelser noteret.
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 på en enkelt underdatabehandleraftale, at denne indeholder samme krav og forpligtelser, som er anført i databehandleraftalen mellem den dataansvarlige og databehandleren.	Ingen afvigelser noteret.

Kontrolmål F:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen afvigelser noteret.
F.6	På baggrund af en ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, foretager databehandleren en 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, tredjelands overførselsgrundlag og lignende. Inspiceret dokumentation for, at information om opfølgning hos underdatabehandlere meddeles den dataansvarlige, således at denne kan tilrettelægge eventuelt tilsyn.	Ingen afvigelser noteret.

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	PwC's udførte test	Resultat af test
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at personoplysninger alene overføres til tredjelande eller internationale organisationer i henhold til aftale med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser noteret.
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. Inspiceret ved en stikprøve på en enkelt dataoverførsel fra databehandlerens oversigt over overførsler, at der er dokumentation for, at overførslen er aftalt med den dataansvarlige i databehandleraftalen eller senere godkendt.	Ingen afvigelser noteret.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Inspiceret, at der foreligger formaliserede procedurer for sikring af et gyldigt overførselsgrundlag. Inspiceret, at procedurerne er opdateret. Inspiceret ved en stikprøve på en enkelt dataoverførsel fra databehandlerens oversigt over overførsler, at der er dokumentation for et gyldigt overførselsgrundlag i databehandleraftalen med den dataansvarlige, samt at der kun er sket overførsler, i det omfang dette er aftalt med den dataansvarlige.	Ingen afvigelser noteret.

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	PwC's udførte test	Resultat af test
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand til den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser noteret.
H.2	Databehandleren har etableret procedurer, som 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.	Inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.	Ingen afvigelser noteret.

Kontrolmål I:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser noteret.
I.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejdere • Overvågning af netværkstrafik • Opfølgning på logning af adgang til personoplysninger.	Inspiceret, at databehandleren udbyder awarenesstræning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Inspiceret dokumentation for, at netværkstrafikken overvåges, samt at der sker opfølgning på anormaliteter, overvågningsalarmer, overførsel af store filer mv. Inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang.	Ingen afvigelser noteret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 24 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Forespurgt, om der har været konstateret sikkerhedsbrud hos underdatabehandlerne, og inspiceret, at disse er anført i oversigten over sikkerhedshændelser.	Ingen afvigelser noteret.

Kontrolmål I:

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

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet. Disse procedurer skal indeholde anvisninger på beskrivelser af: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede anvisninger på: • Beskrivelse af karakteren af bruddet på persondatasikkerheden • Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden • Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.	Ingen afvigelser noteret.

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

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

Torben Stigaard
Kunde
På vegne af: Visma Plandisc A/S
Serienummer: 3f1cf406-0d28-424b-8797-73c45dcb6004
IP: 85.184.xxx.xxx
2024-02-28 13:07:40 UTC

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
På vegne af: PwC
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2024-02-28 13:19:18 UTC

Penneo dokumentnøgle: G01IJ-I3CM0-NXE16-NCNBI-6D2NQ-PJ6TD