www.pwc.dk

EG Danmark A/S

Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger pr. 31. maj 2023 i relation til Bodine i henhold til databehandleraftale med dataansvarlige

Juni 2023

Indholdsfortegnelse

1. Ledelsens udtalelse

EG Danmark A/S behandler personoplysninger på vegne af dataansvarlige i henhold til databehandleraftaler.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlig, der har anvendt udvikling, drift og support af Bodine (Bogeronine, daiaform+, NemForm), 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.

EG Danmark A/S anvender IT Relation A/S som underdatabehandler for hosting. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som IT Relation A/S varetager for EG A/S.

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

EG Danmark A/S bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en tilfredsstillende præsentation af udvikling, drift og support af Bodine, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesreglerne pr. 31. maj 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan informationssikkerhed og foranstaltninger i relation til udvikling, drift og support af Bodine 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 udvikling, drift og support af Bodine 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 udvikling, drift og support af Bodine 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 udvikling, drift og support af Bodine, 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. 31. maj 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, og

(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.

Ballerup, den 13. juni 2023
EG Danmark A/S

Steffen Rugtved
Direktør
EG Digital Welfare

2. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring om informationssikkerhed og foranstaltninger pr. 31. maj 2023 i relationt til Bodine i henhold til databehandleraftale med dataansvarlige

Til: EG Danmark A/S og dataansvarlig

Omfang

Vi har fået som opgave at afgive erklæring om EG Danmark A/S' beskrivelse i afsnit 3 af deres udvikling, drift og support af Bodine i henhold til databehandleraftale med dataansvarlige pr. 31. maj 2023 (beskrivelsen) og om udformningen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Nærværende erklæring omfatter, om EG Danmark A/S har udformet hensigtsmæssige kontroller, der knytter sig til de kontrolmål, der fremgår af afsnit 4. Erklæringen omfatter ikke en vurdering af EG Danmark 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").

EG Danmark A/S anvender IT Relation A/S som underdatabehandler for hosting. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som IT Relation A/S varetager for EG A/S.

Enkelte af de kontrolmål, der er anført i EG Danmark A/S' beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos dataansvarlig er hensigtsmæssigt udformet sammen med EG Danmark A/S' kontroller. Erklæringen omfatter ikke egnetheden 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.

EG Danmark A/S' ansvar

EG Danmark 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.

PricewaterhouseCoopers er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om EG Danmark 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 deres udvikling, drift og support af Bodine 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, egnetheden af de heri anførte mål samt egnetheden 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

EG Danmark 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 udvikling, drift og support af Bodine, 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 udvikling, drift og support af Bodine, således som det var udformet og implementeret pr. 31. maj 2023, 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. 31. maj 2023.

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 EG Danmark A/S' udvikling, drift og support af Bodine, 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, 13. juni 2023
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 77 12 31

Jesper Parsberg Madsen
statsautoriseret revisor
mne26801

3. Beskrivelse af behandling

Indledning og omfang

Denne systembeskrivelse vedrører de generelle it-kontroller i tilknytning til applikationsudvikling og hostingaktiviteter i EG Danmark A/S og EG Digital Welfare ApS, som er ejet af kapitalfonden Francisco Partners. Standard-it-drift og hostingaktiviteter leveres af IT relation A/S, og applikationsudvikling varetages af EG Digital Welfare ApS, som i denne erklæring er benævnt EG.

Hvad angår applikationsudviklingen arbejdes der efter de samme procedurer og metoder på alle udviklingsopgaver hos EG.

EG anvender IT relation A/S som underleverandør af fysisk sikkerhed i datacentre, hvor EG's kunder driftes fra. IT relation A/S er herunder ansvarlig for fysiske sikkerhed, hardware, netværk, backup, hypervisor og storage.

Denne erklæring er udarbejdet efter partielmetoden og inkluderer således ikke kontroller hos underleverandøren IT relation A/S. Disse kontroller dækkes for 2022 ved modtagelse af revisionserklæring fra underleverandørerne.

EG varetager drift og monitorering i forbindelse med it-drift og hostingaktiviteter og er i forbindelse hermed ansvarlig for at sikre implementeringen og funktionen af kontrolsystemer for at forebygge og opdage fejl, herunder bevidste fejl, med henblik på overholdelse af kontrakter og god skik.

Denne beskrivelse er afgrænset til generelle standarder for administration som beskrevet i EG's standardkontrakt. Specifikke forhold, der er relateret til individuelle kundekontrakter, er ikke omfattet.

Med baggrund i den ovenstående afgrænsning og nedenfor nærmere angivne systembeskrivelse vurderer EG, at vi i alle væsentlige forhold har opretholdt effektive kontroller. EG er opmærksom på, at der kontinuerligt sker udvikling inden for området, og EG arbejder kontinuerligt på at forbedre kontrollerne.

EG specialiserer sig i at bygge og levere branchespecifik vertikal software. Denne erklæring omfatter EGs leverancer under kundekontrakter med henblik på EGs overholdelse af sine forpligtelser som databehandler efter Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (Databeskyttelsesforordningen)(refereret til i det følgende som GDPR)

Arbejdet med GDPR er delt i to fokusområder – det interne, som vedrører alle interne processer, hvor vi som virksomhed har med persondata at gøre (eksempelvis HR, it, marketing og økonomi), og det kunderettede, som denne erklæring omfatter, der vedrører alle de områder, hvor vi interagerer med vores kunder og potentielt kunne komme i berøring med persondata.

Beskrivelse af ydelser, der er omfattet af erklæringen

De ydelser, som EG leverer, er tilpasset flere forskellige typer af kunder. Betingelserne for de enkelte kunder er angivet i kontrakter, hvor der for hvert forretningsområde tages udgangspunkt i standardkontrakter, som kan indeholde individuelle tilretninger og optioner. Følgende områder dækker over de ydelser, som EG tilbyder:

Udvikling og vedligehold af applikationssoftware: Omfatter kunder, som får udviklet applikationer hos EG.

Denne erklæring omfatter kun EG Digital Welfare ApS på følgende løsninger og moduler til kunder:

- BorgerOnline
- Diaform+

Der leveres systemer til dataindsamling, primært til landets kommuner, men også til andre offentlige myndigheder som f.eks. Styrelsen for Institutioner og Uddannelsesstøtte. De systemer til dataindsamling, som leveres, fungerer grundlæggende ens og omfatter:

- Diaform+
- Framework til "Ansøgning om Statens Voksenuddannelsesstøtte (SVU)"
- Borgeronline Framework, herunder:
    - Alle KL- og DL-løsninger
    - Medbetjeningsformularer
    - MedarbejderOnlineformularer
    - Selvbetjeningsløsninger tilhørende produkterne Nemform, Vielse og adressefore-spørgsel og Bopælsattest
-

Systemerne behandler almindelige personoplysninger, jf. databeskyttelsesforordningens artikel 6, følsomme personoplysninger, jf. databeskyttelsesforordningens artikel 9 og oplysninger om cpr-nummer, jf. databeskyttelseslovens § 11).

DATAINDSAMLING
Dataindsamling via Diaform+
En sagsbehandler indtaster personoplysninger i en formular og sender denne til en borger. Opslag foretages i Datafordeleren. Formularen sendes signeret via sikker forbindelse til borgerens Digital Post eller via fjernprint i de tilfælde, hvor borgeren ikke har Digital Post. Ønsker sagsbehandleren,
at borgeren skal udfylde oplysninger i den pågældende formular, fremsendes tillige et link til en digital formular, og dataindsamling vil ske som beskrevet i afsnittet om Borgeronline Framework.

Dataindsamling igennem Borgeronline Framework
En bruger (borger/virksomhedsrepræsentant/medarbejder) tilgår en digital formular fra Borgeronline via en sikker forbindelse (https). Den digitale formular kan tilgås fra de mest gængse enheder via en browser med adgang til internettet, f.eks. computer, smartphone og tablet.

Har kunden valgt, at brugeren skal logge ind med MitID/NemID før opstart af formularen, gøres det via den fællesoffentlige brugerstyringsløsning (NemLogIn).

Hvilke felter en given formular indeholder, afgøres af kunden, der enten selv specificerer indholdet i formularen eller anvender KL-blanketpakke. Formularen udfyldes online, og det givne forløb hertil genereres af BorgerOnlines web-server. I løbet af udfyldelse af formularen sendes brugerens indtastede oplysninger via en sikker forbindelse til BorgerOnlines servermiljø hos IT Relation A/S og gemmes i en database.

En stor del af Borgeronline/diaform+ formularer afsluttes med digital signering. Her udveksles de indsamlede oplysninger med Nets DanID, som returnerer oplysninger om brugerens digitale signering af det fremsendte. Sluttelig omdannes formularen og de udfyldte oplysninger til pdf-format. En kopi fremsendes til brugerens digitale postkasse via en sikker forbindelse. Til kunden fremsendes en krypteret e-mail indeholdende både pdf, signeringsbevis og en xml-signatur.

Der kan i formularer desuden foretages opslag i fællesoffentlige services, hvor data hentes med udgangspunkt i de indtastede oplysninger. Opslag foretages via Datafordeleren og CPR-registret. Opslag i CPRregistret og Serviceplatformen sker kun, hvis brugeren logger ind via NemLogIn, og der hentes kun oplysninger om den bruger, der er logget ind. Opslag i fællesoffentlige services sker via en sikker forbindelse,
og der bruges certifikat til identifikation, hvor det påkræves.

I formularer vil der i visse tilfælde også ske opslag i CVR-registret og i en adresseverificeringsservice. Disse oplysninger er frit tilgængelige på Internettet og kræver derfor ikke særligt fokus i relation til informationssikkerhed.

Al data, der er opsamlet via en formular, slettes automatisk fra databasen efter en fastsat tidsperiode.
Ved ophør af databehandlingen træffer kunden beslutning om, hvorvidt der skal ske tidligere sletning eller tilbagelevering af personoplysningerne.

Kontrolmiljø

Ledelsesstruktur

Overholdelse af kravene i relation til IT-Sikkerhed følger den organisation, som er etableret i relation til håndtering af informationssikkerhed som beskrevet nedenfor.

I EG bygger organisationsform og ledelse på en funktionsopdelt struktur. Lederen for den enkelte afdeling har personaleansvar. Sikkerhedsansvaret i de enkelte processer er fordelt på henholdsvis de(n) ansvarlige og de(n) udførende. Den ansvarlige leder har ansvar for at sikre at processen følges og dokumenteres hos de udførende ansatte.

Organisering af informationssikkerhed (kontrolmål B)

Det overordnede ansvar for it-sikkerheden i EG og tilhørende selskaber ligger i it-sikkerhedsudvalget, (EG Security Committee), der behandler alle større relevante it-sikkerhedsspørgsmål af principiel karakter.

It-sikkerhedsudvalget er repræsenteret af medarbejdere fra den øverste ledelse, divisionschefer, leder af IT og CISO, samt leder af Group Legal & Compliance. It-sikkerhedsudvalget refererer direkte til direktionen i EG.

Udvalget er normgivende og fastsætter på grundlag af den vedtagne it-sikkerhedspolitik de principper og retningslinjer, der skal sikre målopfyldelsen.

Medlemmer af it-sikkerhedsudvalget deltager ligesom alle øvrige medarbejdere løbende i relevant awareness træning inden for IT-Sikkerhed. It-sikkerheden er effektueret igennem intern strategi, politikker, standarder, procedurer og guidelines.

VP for Corporate IT er ansvarlig for den operationelle drift i henhold til de udarbejdede retningslinjer og den daglige ledelse.

Det er medarbejdernes daglige leder, der er ansvarlig for at følge op på, at medarbejderen overholder koncernrelaterede politikker og procedurer, der understøtter it-sikkerhedspolitikken, samt lokale retningslinjer og procedurer.

Sikkerhedshændelser status og sikkerhedssvagheder rapporteres til it-sikkerhedsudvalget, hvor evt. yderligere tiltag initieres.

GDPR-udvalg (GDPR Committee)

Det overordnede ansvar for databeskyttelsesspørgsmål af principiel karakter varetages af EG's GDPR-udvalg (GDPR Committee).

GDPR-udvalget (GDPR Committee) er et normgivende udvalg for EG's strategi og risici i forhold til GDPR-relaterede emner. Udvalget understøtter og sikrer effektiv virksomhed samt bedste praksis indenfor databeskyttelse på tværs af EG Danmark A/S og tilhørende selskaber.

Formanden for GDPR-udvalget udpeges af CFO og vælges blandt udvalgets medlemmer. Derudover vælges en sekretær for udvalget blandt de ansatte i Group Legal & Compliance.

GDPR-Udvalget (GDPR Committee) fastsætter gældende databeskyttelsesretlige principper og retningslinjer i overensstemmelse med GDPR og anden national databeskyttelseslovgivning samt foranlediger GDPR-initiativer, faciliterer relevant awareness & training og sikrer en optimal revisionsproces (ISAE 3402 og ISAE 3000).

Uddannelse og træning
Når politikker, retningslinjer procedurer (standard operating procedures) opdateres, kommunikeres dette til alle medarbejdere. Politikker og procedurer er tilgængelige i EG's ISMS system, , hvor medarbejderne altid kan orientere sig. Hvis medarbejdere bliver opmærksomme på fejl og mangler, sker tilbagemelding til den relevante kontaktperson eller afdeling listet i den pågældende politik eller procedure.

Efterlevelse af instruks fra den dataansvarlige (Kontrolmål A)

EG har etableret en række GDPR-politikker og procedurer, som medarbejderne har modtaget og er trænet i efterlevelse af. Disse består bl.a. af:

- GDPR Handbook for employees
- Code of Conduct Employees
- Whistleblower Scheme
- E-mail policy
- Privacy & Cookie Policy
- GDPR-relaterede procedurer (SOP)

EG behandler persondata i overensstemmelse med kundens instruks.EG behandler ikke persondata uden indgået databehandleraftale med den dataansvarlige (kunden). EG har en standard databehandleraftale, der opdateres minimum én gang årligt af Group Legal & Compliance. EGs Standard databehandleraftalen er baseret på det danske datatilsyns skabelon. Hvert løsningsområde skal udarbejde en databehandleraftale med afsæt i EGs standard databehandleraftale indeholdende definerede krav til behandling af persondata herunder:

- Formål med behandlingsaktivitet(er)
- Kategorier af persondata
- Underdatabehandlere
- Overførsel til tredjeland

Brug af underdatabehandlere til udførelse af specifikke behandlingsaktiviteter på vegne af kunden foretages alene efter kunden har godkendt brugen af underdatabehandleren. EG har i databehandleraftalen sikret at alle underdatabehandlere overholder tilsvarende databeskyttelsesretlige forpligtelser som dem fastsat i databehandleraftalen mellem EG og kunden.

For hvert løsningsområde og tværgående proces jf. de forrige afsnit er der etableret passende tekniske og organisatoriske kontroller på områderne.

Der foretages løbende vurdering af, og mindst én gang årligt, om EG fortsat har de nødvendige passende tekniske og organisatoriske sikkerhedsforanstaltninger på plads til fortsat at kunne levere den pågældende løsning og ydelse til kunden.

Tekniske og organisatoriske foranstaltninger (Kontrolmål B og C)

I relation til tekniske og organisatoriske kontroller henvises til de udarbejdede ISAE 3402-erklæringer. Disse omfatter områder som:

- Medarbejdersikkerhed
- Styring af sikkerhedshændelser
- Eksterne parter og leverandørforhold
- Fysisk sikkerhed
- Driftsprocedure
- Overvågning og logning

- Funktionsadskillelse
- Kryptering
- Backup og restore
- Fejlrettelser og support
- Adgangsstyring
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Anskaffelse, udvikling og vedligeholdelse af applikationer
- Katastrofeberedskabsplaner

Udvikling, test og vedligeholdelse:
Personoplysninger, der anvendes til udvikling, test eller lignende, er som udgangspunkt i pseudonymiseret eller anonymiseret form.

Anvendelse sker alene for at varetage kundens formål i henhold til aftale og på dennes vegne.
Der kan i visse tilfælde være behov for at teste på rigtige data, hvor der kan ske overførsel af persondata fra produktion til testmiljø og i den forbindelse indhentes godkendelse hos kunden.

Organiseringen af databeskyttelse og Databeskyttelsesrådgiveren:
EG har ikke en Databeskyttelsesrådgiver, da den primære aktivitet for kerneforretningen i koncernen ikke omfatter behandling af persondata. EG har i stedet et Data Protection Office, der er forankret i EGs juridiske afdeling, Group Legal & Compliance. Afdelingen varetager generelle juridiske opgaver indenfor it, GDPR og compliance.

Databehandler bistår den dataansvarlige:
I det omfang EG forestår behandling af persondata på vegne af og efter instruks fra den dataansvarlige, bistår EG den dataansvarlige med at sikre overholdelsen af:

- forpligtelsen til at gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et niveau, der er tilpasset de risici, der er forbundet med behandlingen
- forpligtelsen til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet) uden unødig forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet, medmindre det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder
- forpligtelsen til – uden unødig forsinkelse – at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
- forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
- forpligtelsen til at høre tilsynsmyndigheden (Datatilsynet) inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko pga. mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

Sletteprocedure (Kontrolmål D)

EG har skriftlige procedurer for sletning af persondata i overensstemmelse med den indgåede databehandleraftale med kunden.

Særlige krav til sletning af persondata, herunder sletterutiner, følger specifikt af databehandleraftalen indgået med kunden.

Ved ophør af behandling af persondata for den dataansvarlige vil EG enten tilbagelevere persondata til den dataansvarlige og/eller slette persondata, hvor dette ikke er modstridende med anden lovgivning. Nærmere procedure for ophør af behandling af persondata aftales efter kundens instruks i overensstemmelse med databehandleraftalen med kunden.

Opbevaringsprocedure (Kontrolmål E)

EG har skriftlige procedurer for opbevaring af persondata i overensstemmelse med den indgåede databehandleraftale med kunden.

Særlige krav til opbevaring og sletning af persondata, herunder opbevaringsperioder, følger specifikt af databehandleraftalen indgået med kunden.

Oversigt over behandlingsaktiviteter samt angivelse af lokaliteter, lande og landområder for EG som databehandler og dennes underdatabehandlere følger af databehandleraftalen indgået med kunden.

Underdatabehandlere (Kontrolmål F)

EG har indgået databehandleraftaler med alle underdatabehandlere for at sikre de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen med kunden. EG anvender kun underdatabehandlere til behandling af persondata ved specifik eller generel godkendelse fra dataansvarlig.

EG fører en oversigt over alle godkendte underdatabehandlere omfattende som minimum den enkelte underdatabehandlers navn, CVR-nr. eller lignende, adresse og beskrivelse af behandlingsaktivitet.

Nye underdatabehandlere i EG

Alle nye underdatabehandlere i EG bliver vurderet og godkendt af EG's Vendor Approval Board (VAB).

VAB består af VP Procurement, CTO og General Counsel fra Group Legal & Compliance

Derudover vælges en sekretær for VAB blandt de ansatte i Group Legal & Compliance.

VAB sikrer en fælles godkendelsesproces for alle underdatabehandlere, samt sikre at underdatabehandlerne overholder EG's krav i forhold til teknologi, sikkerhed, compliance og databeskyttelse.

Tilsyn med underdatabehandlere

EG foretager tilsyn med alle underdatabehandlere mindst én gang årligt baseret på en risikovurdering. Tilsyn med underdatabehandlere foretages centralt i EGs juridiske afdeling, Group Legal & Compliance. Tilsynet sikrer og dokumenterer de anvendte underdatabehandlere til den ydelse som EG leverer til kunden i forhold til:

- GDPR-compliance herunder sikre en tilstrækkelig beskyttelse af de registreredes rettigheder i overensstemmelse med GDPR, hvis persondata behandles
- Lever op til tilsvarende tekniske sikkerhedsforanstaltninger som indeholdt i databehandleraftalen med kunden

- Lever op til tilsvarende organisatoriske sikkerhedsforanstaltninger som indeholdt i databehandleraftalen med kunden

Alle endelige godkendelser af tilsynsrapporter på underdatabehandlere foretages af VAB.

Overførsel til tredjeland eller internationale organisationer (Kontrolmål G)

Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med databehandleraftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.

Den registreredes rettigheder (Kontrolmål H)

Under hensyntagen til behandlingens karakter bistår EG 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 i henhold til GDPR.

EG har en procedure for håndtering og dokumentation af henvendelser fra dataansvarlige i relation til bistand til håndtering af de registreredes rettigheder (indsigtsret, sletning, berigtigelse mv.).

Nærmere procedure og kontroller for håndtering og dokumentation for bistand til den dataansvarlige følger af den indgåede databehandleraftale mellem EG og kunden.

Procedure for håndtering af sikkerhedsbrud (Kontrolmål I)

EG er som databehandler forpligtet til at underrette den dataansvarlige ved brud eller eventuelle brud på persondatasikkerheden i overensstemmelse med databehandleraftalen efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden hos EG eller dennes underdatabehandler.

EG bistår som databehandler den dataansvarlige i forbindelse med indberetning af databrud til Datatilsynet.

Komplementerende kontroller hos de dataansvarlige

Som led i levering af ydelserne er der kontroller, som forudsættes implementeret af de dataansvarlige, og som er væsentlige for at opnå de kontrolmål, der er anført i beskrivelsen. Dette omfatter bl.a.:

- Stillingtagen til konsekvenser i relation til persondatabeskyttelse, når der ændres i eksisterende løsninger (privacy by design og privacy by default) og fremsættelse af ændringsanmodning hertil til EG i relevant omfang
- Stillingtagen til / test af nye versioner af løsninger ifm. implementering (change management)
- Opsætning og styring af egne brugere i løsningen i produktionsmiljøet (identity and access management)
- Opsætning og styring af brugere fra EG, som har adgang til kundens miljø (identity and access management)

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 bemærkninger.
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 bemærkninger.
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 bemærkninger.

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 bemærkninger.
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 bemærkninger.
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 bemærkninger.
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 bemærkninger.

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 bemærkninger.
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 bemærkninger.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.	Ingen bemærkninger.

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.	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 bemærkninger.

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.
			Vi har konstateret, at logning på servere ikke er tilstrækkelig på alle parametre.
			Ingen yderligere bemærkninger.

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 bemærkninger.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	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 bemærkninger.
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 udtræk af tekniske sikkerhedsparametre og -opsætninger, at systemer, databaser og netværk er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.	Ingen bemærkninger.

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, herunder 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 bemærkninger.
B.14	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.	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 bemærkninger.
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 bemærkninger.

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 bemærkninger.
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 bemærkninger.
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 bemærkninger.

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 bemærkninger.
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 bemærkninger.
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 bemærkninger.

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 bemærkninger.

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 bemærkninger.
D.2	Eventuelle specifikke krav til databehandlerens opbevaringsperioder og sletterutiner fremgår af databehandleraftaler.	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 bemærkninger.
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 bemærkninger.

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 bemærkninger.
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 bemærkninger.

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 bemærkninger.
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 bemærkninger.
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 bemærkninger.
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 bemærkninger.

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 bemærkninger.
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 bemærkninger.

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.	Der er ikke overførsel til tredjeland. Ingen yderligere bemærkninger.
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.	Der er ikke overførsel til tredjeland. Ingen yderligere bemærkninger.
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.	Der er ikke overførsel til tredjeland. Ingen yderligere bemærkninger.

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 bemærkninger.
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 bemærkninger.

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 bemærkninger.
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 awareness-træning 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 bemærkninger.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 72 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 bemærkninger.

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 bemærkninger.

PENNEO

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."

Steffen Rugtved
EG Digital Welfare ApS CVR: 27720102
Kunde
På vegne af: EG Danmark A/S
Serienummer: 5fabc722-0f9c-4471-a9d1-4e29fa5e772d
IP: 185.128.xxx.xxx
2023-06-13 06:00:19 UTC

Mit ID

Jesper Parsberg Madsen
Statsautoriseret revisor
Serienummer: d928e935-d26a-4251-b316-bc64d31db8a2
IP: 83.136.xxx.xxx
2023-06-13 06:08:00 UTC

Mit ID

Penneo dokumentnøgle: SEIMZ-4U2DV-4OQPG-UEAG4-83402-DZTEJ