bakertilly

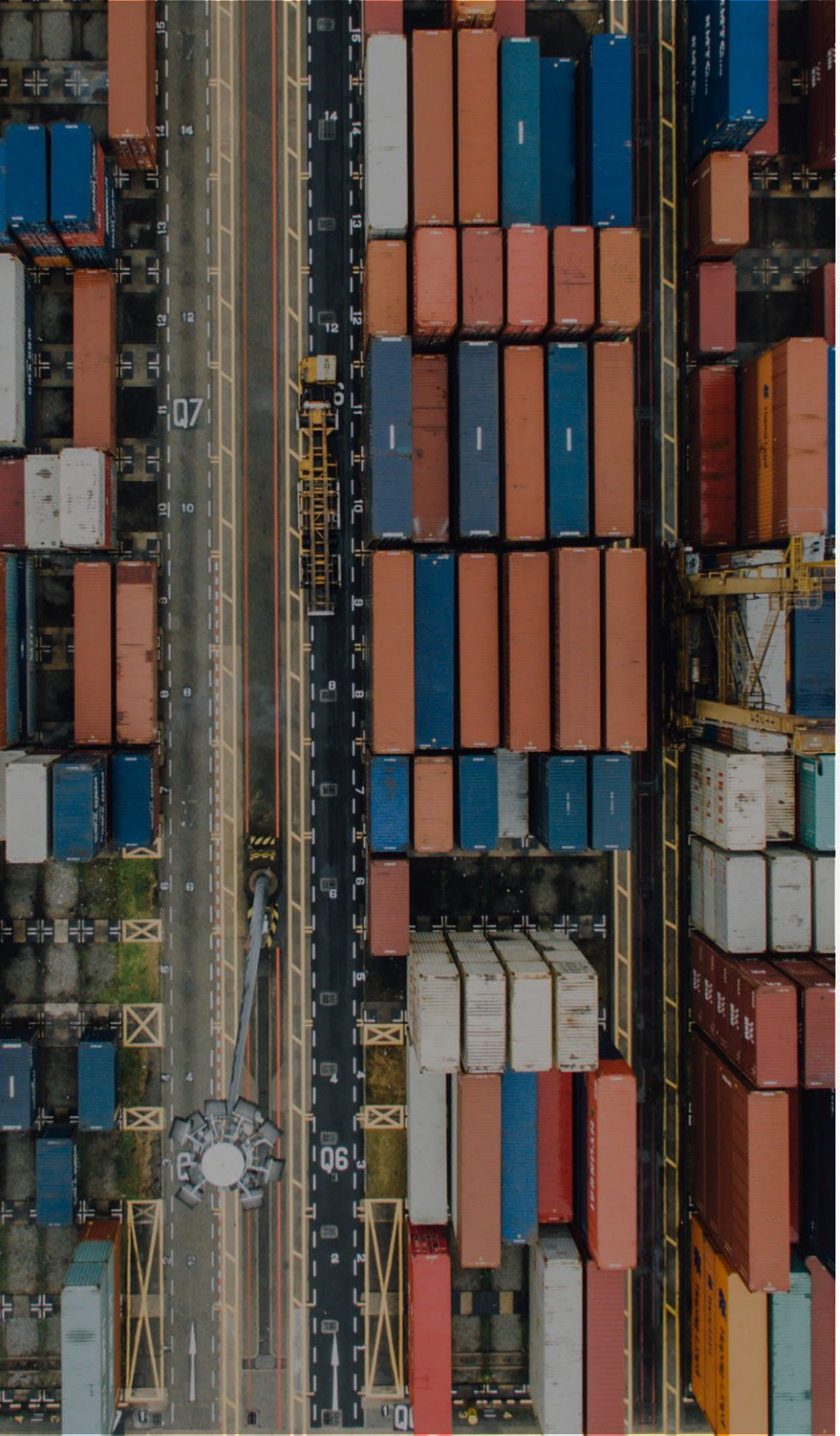
RÅDGIVNING • SKAT • REVISION

G4S Security Services A/S

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i forhold til databehandleraftale

Pr. 28. august 2024

Now, for tomorrow



Indholdsfortegnelse

1	Ledelsens udtalelse	Side	2
2	Uafhængig revisors erklæring	Side	4
3	Beskrivelse af behandling	Side	6
4	Kontrolmål, kontrolaktivitet, test og resultat heraf	Side	8

1. Ledelsens udtalelse

G4S Security Services A/S CVR-nr. 26 89 12 80 behandler personoplysninger på vegne af kunder i henhold til de indgåede databehandleraftaler dækkende de konkrete ydelser, der leveres til den enkelte kunde.

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt G4S Security Services A/S, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") er overholdt. G4S Security Services A/S bekræfter, at:

a) Den medfølgende beskrivelse, giver en retvisende beskrivelse af G4S Security Services A/S, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen pr. 28. august 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   i. Redegør for, hvordan ydelserne var udformet og implementeret, herunder redegør for:

      - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
      - De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger
      - 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 underrettelse til de registrerede
      - De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet
      - Kontroller, som vi med henvisning til ydelsernes afgrænsning, har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen
      - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger

1. Ledelsens udtalelse (fortsat)

ii. Indeholder relevante oplysninger om ændringer ved databehandlerens ydelse til behandling af personoplysninger foretaget pr. 28. august 2024.

iii. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne sikkerhedstiltag 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 ydelserne, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

b. De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var efter vores vurdering hensigtsmæssigt udformet og fungerede effektivt pr. 28. august 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, og

III. Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse pr. 28. august 2024.

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

I relation til ovenstående vurderinger bemærkes, at reguleringen vedrørende behandling af persondata er ny og kompleks. Der har endnu ikke på alle områder udviklet sig en konsistent praksis for hvordan de enkelte regler skal fortolkes. Selvom det er vores vurdering, at vi har etableret og opretholdt passende tekniske og organisatoriske foranstaltninger, kan der således vise sig at være forhold, hvor myndigheder og samarbejdspartnere anlægger en anden vurdering.

Albertslund, den 23. oktober 2024

Ole Knudsen

Adm. direktør

2. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med G4S Security Services A/S' kunder relateret til ydelsen.

Til: G4S Security Services A/S og G4S Security Services A/S' kunder relateret til ydelsen

Omfang

Vi har fået som opgave at afgive erklæring om G4S Security Services A/S' beskrivelse af ydelsen i henhold til databehandleraftale med dataansvarlige, pr. 28. august 2024, og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med begrænset sikkerhed.

G4S Security Services A/S' ansvar

G4S Security Services A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse, 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, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Baker Tilly Denmark Godkendt Revisionspartnerselskab 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.

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.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om G4S Security Services A/S' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger og yderligere krav ifølge dansk revisorlovgivning, med henblik på at opnå begrænset sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

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

2. Uafhængig revisors erklæring (fortsat)

Omfanget af de handlinger vi har udført, er mindre end ved en erklæringsopgave med høj grad af sikkerhed. Som følge heraf er den grad af sikkerhed, der er for vores konklusion, betydeligt mindre end den sikkerhed, der ville være opnået, hvis der var udført en erklæringsopgave med høj grad af sikkerhed.

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

Begrænsninger i kontroller hos en dataansvarlig

G4S Security Services 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 ydelsen, som hver enkelt dataansvarlig måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

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. Under vores arbejde er vi ikke blevet bekendt med forhold, der giver os anledning til at konkludere,

a) at beskrivelsen af ydelsen, således som denne var udformet og implementeret pr. 28. august 2024, ikke i alle væsentlige henseender er retvisende, og
b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, ikke i alle væsentlige henseender var hensigtsmæssigt udformet pr. 28. august 2024, og
c) at de vurderede kontroller, som var de kontroller, der var nødvendige for at give begrænset sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, ikke har fungeret effektivt pr. 28. august 2024.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev vurderet (ved analyse og forespørgsel), samt arten, den tidsmæssige placering og resultater af disse vurderinger fremgår i afsnit 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af vurdering af kontroller er udelukkende tiltænkt dataansvarlige, der har anvendt G4S Security Services A/S' ydelse, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

København, den 23. oktober 2024

Baker Tilly Denmark
Godkendt Revisionspartnerselskab
CVR-nr. 35 25 76 91

Michael Brink Larsen
statsautoriseret revisor
MNE-nr. mne23256

3. Beskrivelse af behandling

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er at levere sikkerhedsydelser i overensstemmelse med hovedaftalen mellem databehandleren og den dataansvarlige. Databehandleren vil, til brug for at levere den aftalte ydelse og efter nærmere aftale med den dataansvarlige, behandle og opbevare data. Denne erklæring omfatter alene systemerne Milestone, Symmetry, SPC, S25 og Stages. Denne erklæring omfatter således ikke databehandlerens øvrige produkter eller interne processer og systemer som f.eks. HR, IT, marketing, økonomi m.v.

Databehandleren har et stort fokus på GDPR og følger løbende udviklingen inden for GDPR, og sørger i forbindelse hermed løbende for at opdatere kontroller, politikker og processer. Databehandleren har desuden en Data Protection Officer med det overordnede ansvar for at sikre overholdelse af GDPR.

Karakteren af behandlingen

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige afhænger af typen af produkt samt opsætning ift. hosting.

Milestone er et videoovervågningssystem, hvortil der kan kobles et ubegrænset antal af kameraer, samt avancerede funktioner som f.eks. people counting.

Symmetry er et adgangskontrolsystem, som sektionere og begrænser adgang til sikrede områder via fx adgangskort.. Symmetry kan desuden bruges til f.eks. gæsteregistrering.

SPC er et tyverialarmsystem, som detekterer indbrud og videregiver disse oplysninger til G4S' kontrolcentral.

S25 er en overbygning som kan sammenkæde flere tyverialarmsystemer og via fx PC give brugeren overblik og en intuitiv og brugervenlig betjening.

Stages er det system, der benyttes på G4S kontrolcentral til monitorering af tyverialarmer og videoovervågning.

De ydelser, som databehandleren 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 databehandleren tilbyder:

On premise

Sikringssystemer og ydelser, hvor alle data opbevares og administreres lokalt hos den respektive kunde (den dataansvarlige).

On premise med WEB-client

Sikringssystemer og ydelser, hvor alle data opbevares og administreres lokalt hos den respektive kunde (den dataansvarlige) og hvor der er tilknyttet en WEB-client, der anvendes som fx kundens betjeningspanel eller overvågning.

3. Beskrivelse af behandling (fortsat)

Karakteren af behandlingen (fortsat)

Hosting/Cloud - eventuelt med WEB-client

Sikringssystemer og ydelser, hvor data hostes for kunden hos en anden end kunden (den dataansvarlige), nemlig hos databehandleren eller i en Cloudløsning hos en af databehandlerens leverandører.

Alle ovenstående tre områder kan have en eller flere af følgende set-ups:

- Uden overførsel af signaler eller data til databehandlerens kontrolcentral.
- Med overførsel af signaler eller data til databehandlerens kontrolcentral, fx tyverialarmsignaler, billeder eller video til brug for reaktion jf. kontraktlig aftale.
- Med overførsel af signaler eller data til en af databehandlerens underleverandører (underdatabehandler), fx tyverialarmsignaler, billeder eller video til brug for reaktion jf. kontraktlig aftale.

Personoplysninger

Databehandleren kan alt efter produkt- og ydelsestype behandle oplysninger om navn, telefonnummer, e-mailadresse eller informationer, som den dataansvarlige selv vælger at notere i produkternes brugersoftware samt videooptagelser.

Databehandleren behandler ikke følsomme personoplysninger og opfordrer databehandleren til ikke selv at notere sådanne i produkternes brugersoftware.

Kategorier af registrerede personer omfattet af databehandleraftalen:

- Ansatte
- Kunder
- Besøgende på kundens adresse
- Ved video omfatter behandlingen alle personer som indfinder sig på det sikrede område

3. Beskrivelse af behandling (fortsat)

Risikovurdering

Databehandleren udfører løbende risikovurderinger for systemer og processer. Der gives i denne forbindelse en risikoscore, hvorefter databehandleren vurderer de risici, som der er forbundet med behandlingen samt eventuelle risikominimerende tiltag.

Databehandleren foretager ikke højrisiko databehandling.

For de systemer som er omfattet af denne erklæring, anses risikoen for de registreredes rettigheder som lav, og der er foretaget omfattende kontrolforanstaltninger for at sikre de registreredes rettigheder.

Kontrolforanstaltninger

1. Efterlevelse i overensstemmelse med den indgåede databehandleraftale

Databehandleren har skriftlige procedurer, der beskriver, hvornår, hvorfor og hvordan der indgås databehandleraftaler, jf. artikel 28, stk. 3. Proceduren opdateres løbende efter behov.

Behandling af personoplysninger i databehandleraftaler udføres udelukkende jf. den aftalte instruks.

2. Tekniske foranstaltninger til sikring af relevant behandlingssikkerhed

Bag personoplysninger, der er i databehandlerens varetægt, og som er nødvendige for, at databehandleren kan udføre sine kontraktlige forpligtelser over for kunder (dataansvarlige) ligger følgende tekniske foranstaltninger:

3. Interne systemer og interne kundevendte systemer

Databehandleren anvender ”defence-In-depth" teknologier dvs. flere lag af forsvar for at beskytte data, bl.a. fysisk sikkerhed, stærk kryptering, uafhængige sikkerhedsforanstaltninger, sikkerhedsovervågning, stærk brugergodkendelse og andre kontroller, der effektivt beskytter data i nøglesystemer.

For hvert system er der foretaget risikovurderinger. Disse opdateres løbende.

4. Tilgængelighed og robusthed

Databehandleren anvender IT sikkerhedsstyringskontroller, der bl.a. beskytter mod malware downloads, samt forhindrer besøg af websites med potentielt skadeligt indhold, brugergruppekontrol og konfigurationer. Endvidere foretages løbende tests og kontroller for systemers sårbarhed. Servere samt klienter sikkerhedspatches systematisk.

Driftsmiljøet overvåges 24/7/365 via en automatiseret service. Der overvåges ressourcer for servere (Cpu, ram, disk, netværk) og tilgængelighed. Overvågningen omfatter også relevante it-services; eksempelvis back-ups, tilgængelighed for kundevendte systemer og systemer til internt brug.

Ved eventuelle fejl rapporteres til databehandlerens Network Operation Center, hvor denne bliver undersøgt. Er der tale om kritiske fejl i servere eller services, adviseres den vagthavende driftsmedarbejder direkte.

3. Beskrivelse af behandling (fortsat)

Kontrolforanstaltninger (fortsat)

Databehandleren foretager regelmæssige sårbarhedsvurderinger af højrisikosystemer og forebygger i nødvendigt omfang. Individuelle applikationer som implementeres af databehandleren og gennemgår penetrationstest af enten leverandør eller uvildigt firma, alt afhængigt af systemets sikkerhedsrisikoprofil.

Endvidere foretager databehandleren systematisk sårbarhedsscanninger af internt netværk, såvel som offentlige IP adresser, webservere m.m.

5. Infrastruktur, adgangssikkerhed og sporbarhed

Databehandlerens logiske sikring afføder, at kun autoriserede brugere har adgang til IT-systemer.

Alle systemer er adgangsbegrænset og -kontrolleret. Det betyder, at adgange til systemer er styret, så de kun kan tilgås af medarbejdere med legalt formål samt at adgange fratages medarbejdere, når der ikke længere er et legalt formål. Der udføres regelmæssige kontroller af adgange.

Tildeling af adgang til driftsmiljø sker i overensstemmelse med forretningsbetingede formål og informationernes klassifikation. Både fysisk og logisk adgang er baseret på principperne "need-to-know" og "least privilege", hvor der tildeles adgang til de informationer, hvortil man har behov for at kunne udføre sine opgaver, sit job eller sin rolle.

Anmodning om adgang til interne IT-systemer og produktionsmiljøer følger en fastlagt procedure, der sikrer en adskillelse i anmodning, godkendelse, verifikation og implementering. Adgangsstyringen dokumenteres i et centralt system.

Alle IT-medarbejdere har underskrevet en Code Of Conduct til efterlevelse.

Databehandlerens infrastruktur består af to datacentre som er placeret på to af hinanden uafhængige adresser. Der er redundans imellem de to sites, både på netværk og serverdrift. Begge datacentre er sikret af UPS/Nødstrømsgenerator anlæg samt Automatiske IndbrudsAlarmanlæg (AIA), TV-overvågning (ITV), AdgangsKontrolanlæg (ADK), Automatiske BrandAlarmanlæg (ABA) og brandbekæmpelsesanlæg.

Logning anvendes til overvågning, fejlhåndtering og efterforskning. Da logs indeholder mange forskellige informationer, har databehandleren også adgangsstyring til logs afhængigt af, hvilke opgaver den enkelte medarbejder må udføre.

Databehandleren arbejder med logning på flere niveauer:

- Applikationslogs, der håndterer specifikke operationer i applikationer,
- Adgangslogs, der logger, hvornår brugere logger ind i applikationer, logning af, hvilke brugere der tilgår information af følsom og fortrolig karakter i vores applikationer og
- Syslog, som er overvågningslogning.

3. Beskrivelse af behandling (fortsat)

Kontrolforanstaltninger (fortsat)

iii. Databehandlerens kontrolcentral

Databehandleren har en primær kontrolcentral samt en backup kontrolcentral placeret på to af hinanden uafhængige adresser. Begge kontrolcentraler er godkendt af Rigspolitiet i henhold til Lov om Vagtvirksomhed og er omfattet af Rigspolitiets kontroller. Ligeledes er begge kontrolcentraler sikret af både mekanisk, el-teknisk og elektronisk udstyr.

b. Sikringssystemer on premise

Databehandlerens opdrag er alene at foretage installation, service og/eller drift af sikringssystemer og ydelser.

De oplysninger databehandleren har adgang til i forbindelse med installation, servicering og drift af sikringssystemer installeret hos kunder, er de oplysninger kunden vælger at lægge ind i systemerne eller som systemerne genererer i henhold til funktionsformålet. Dette kan være kategorier såsom foto/video, navne, logs etc.

Disse oplysninger kan under visse betingelser tilgås af databehandlerens medarbejdere, som er specieluddannet til at kunne installere, servicere og drifte specifikke systemer. På sikringssystemer med overførsel/forbindelse til databehandlerens kontrolcentral vil oplysninger under visse betingelser kunne ses af databehandlerens kontrolcentralmedarbejdere og behandles, alt efter karakteren af aftalen mellem kunden og databehandleren.

På sikringssystemer, hvor databehandleren behandler personoplysninger, er behandlingen reguleret i en databehandleraftale, med kunden som den dataansvarlige.

c. Sikringssystemer Hosting/Cloud

Databehandleren stiller krav til underleverandører, der leverer systemer - fx sikringssystemer - og ydelser, herunder hosting- og cloudløsninger, om overholdelse af Databeskyttelsesloven/Databeskyttelsesforordningen.

Før en underleverandør antages, foretages der risikovurdering ud fra systemets sikkerhedsklassificering.

Behandles personoplysninger uden for databehandleren, fx af en underleverandører, indgås der en databehandleraftale med denne.

Underleverandører skal efterleve databehandlerens Supplier Code of Conduct. Hører underleverandøren under ydelsesområdet “Hosting/Cloud” tilsikrer databehandleren, at underleverandøren lever op til databeskyttelseskravene via skriftlige tilsyn eller revisorerklæringer fx ISAE3000.

3. Beskrivelse af behandling (fortsat)

Kontrolforanstaltninger (fortsat)

3. Organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed

a. Politikker, procedurer og organisering

Databehandleren har politikker og procedurer for overholdelse af bl.a. Databeskyttelseslovgivningen og andre lovgivninger. Disse er tilgængelige for databehandlerens ansatte sammen med templates og FAQs på databehandlerens interne intranet.

Alle relevante medarbejdere er trænet i og informeret om kravene i lovgivningen og hvordan kravene udleves i praksis via procedurer og kontroller.

Databehandlerens primærpolitikker på GDPR-området er:

- Privatlivspolitik
- Politik om beskyttelse af persondata for medarbejdere og konsulenter
- Politik for opbevaring og sletning af persondata
- Politik for håndtering af brud på persondatasikkerheden
- PC-, mobil-, internet- og mailpolitik
- IT Sikkerhedspolitik
- Dertil hører både informationsmateriale, procedurer og templates, eksempelvis:
- de registreredes rettigheder, herunder ret til indsigt, berigtigelse, sletning, begrænsning af behandlinger og dataportabilitet
- intern audit
- tilsyn med underleverandører

3. Beskrivelse af behandling (fortsat)

Kontrolforanstaltninger (fortsat)

- behandlingssikkerhed, herunder Privacy by design/default
- risiko- og konsekvensvurdering
- indgåelse af databehandleraftaler
- databrud

Politikker og procedurer vurderes løbende i henhold til det definerede interne årshjul.

a. Sikkerhedsforanstaltning for medarbejdere

Samtlige medarbejdere hos databehandleren politigodkendes af Rigspolitiet efter bestemmelserne i Lov om Vagtvirksomhed og ansattes baggrund kontrolleres både før og under ansættelsen hos databehandleren for bl.a. anmærkningsfri straffeattest.

Ligeledes er alle medarbejdere underlagt en kontraktlig tavshedspligt.

b. Awareness

Der gennemføres løbende awareness-træning af medarbejdere i relation til IT- og databehandlingssikkerhed samt Business Contingency. Træning er tilpasset i indhold og hyppighed til respektive medarbejdergrupper.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

4.1 Formål og omfang

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 – Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger.

Vores vurdering af kontrollernes design, funktionalitet og implementering har omfattet kontroller, som vi har vurderet nødvendige for at kunne opnå begrænset sikkerhed for, at de anførte forhold jf. afsnit 4.3 er efterlevet pr. den 28. august 2024. Yderligere kontrolmål- og aktiviteter hos tilsluttede virksomheder omfattes ikke af vores testhandlinger.

Forordningens krav og regler kan ikke fraviges, men forordningen skal omfatte og tage hensyn til formål, behandlingens karakter samt kategorien af personoplysninger mv. på alle niveauer, og den er som følge heraf af mere generel og overordnet karakter på flere områder. Implementeringen af sikkerheden kan således efter partnernes valg tilpasses til den enkelte aftale. Enkelte kundekontrakter kan således også have en rækkevidde, der går ud over databeskyttelsesforordningens eller databeskyttelseslovens almindelige krav. Sådanne yderligere krav er ikke omfattet af nedenstående.

4.2 Udførte testhandlinger

Vi har i forbindelse med udførelsen af vurdering af kontrolaktiviteter udført følgende handlinger:

Metode	Beskrivelse
Forespørgsler	Egnet personale er forespurgt om udførelsen af væsentlige kontrolaktiviteter.
Inspektion	De af kunden fastsatte procedurer, politikker samt dokumentation, er gennemgået og blevet taget stilling til, med henblik på at vurdere, om hvorvidt de konkrete kontroller er designet og implementeret, så de må forventes at blive effektive. Vi har i de tekniske platforme, heri databaser, netværkskomponenter mv, testet den specifikke systemsætning, for at påse om hvorvidt kontrollerne er designet, implementeret og effektive. Dertil er det vurderet om, hvorvidt kontrollerne er overvåget tilstrækkeligt samt i passende intervaller.
Observation	Observation af kontrollernes udførelse.
Genudførelse af kontrol	Vi har selv udført eller observeret en gentagen udførelse af kontrollen, med det formål at verificere, at kontrollen fungerer som antaget.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

4.3 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	Baker Tillys 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 en gang årligt – vurdering af, om procedurerne skal opdateres.	Forespurgt om der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Forespurgt om hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget. Inspiceret oversigt over skriftlige procedurer og vurdereret om denne forekommer opdateret og tilstrækkelig i forhold til databehandlingens omfang.	Ingen anmærkninger.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Forespurgt om hvordan ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks, og vurderet hensigtsmæssigheden heraf. Inspiceret dokumentation for, at ledelsen har foretaget vurdering af databehandlingen efterleves af databehandleren og underdatabehandlere.	Ingen anmærkninger.
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.	Forespurgt om der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Forespurgt om der forligger formaliserede procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Vurderet om det er sandsynligt, at der vil ske underretning af den dataansvarlige hvis instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Kontrolmål B:

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

Nr.	Databehandlerens kontrolaktivitet	Baker Tillys udførte test	Resultat af test
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Forespurgt om der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Forespurgt om hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget. Inspiceret oversigt over skriftlige procedurer og vurdereret om denne forekommer opdateret og tilstrækkelig i forhold til aftalte sikringsforanstaltninger.	Ingen anmærkninger.
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	Forespurgt om der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed. Forespurgt om den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Forespurgt databehandler om hvilke tekniske foranstaltninger der er implementeret, og hvordan disse sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Inspiceret dokumentation for at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med en enkelt udvalgt dataansvarlig.	Ingen anmærkninger.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Forespurgt om der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus software. Inspiceret dokumentation for at antivirus software er installeret og opdateret på et system og en database.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Nr.	Databehandlerens kontrolaktivitet	Baker Tillys udførte test	Resultat af test
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Forespurgt om ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Inspiceret dokumentation for at den seneste kontrol af at firewallen konfigureret i henhold til intern politik herfor.	Ingen anmærkninger.
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 vurdering af om segmentering er behørig.	Ingen anmærkninger.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Forespurgt om der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Forespurgt om der foreligger formaliserede procedurer for periodisk opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Inspiceret dokumentation for at periodisk opfølgning er udført efter planen. Inspiceret for en enkelt bruger for hver gruppe af brugere at brugeres adgange til systemer og databaser, at de er begrænset til medarbejdernes arbejdsbetingede behov.	Ingen anmærkninger.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter: • Enheder • Systemer • Databaser	Forespurgt om der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering. Inspiceret for en tilfældig udvalgt alarm, at der er sket opfølgning, samt at forholdet er meddelt de dataansvarlige i behørigt omfang.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Nr.	Databehandlerens kontrolaktivitet	Baker Tillys udførte test	Resultat af test
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Forespurgt om 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. Forespurgt om teknologiske løsninger til kryptering har været tilgængelige og aktiveret på erklæringstidspunktet. Inspiceret opsætning af enkelte tilfældigt udvalgte transmissions veje at kryptering er effektiv. Forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger på erklæringstidspunktet, samt om de dataansvarlige er behørigt orienteret herom.	Ingen anmærkninger.

B.9	Der er etableret logning i systemer, databaser og netværk af følende forhold:
	
	• Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder
	• Sikkerhedshændelser omfattende:
	  ○ Ændringer i logopsætninger, herunder deaktivering af logning
	  ○ Ændringer i systemrettigheder til brugere
	  ○ Fejlede forsøg på log-on til systemer, databaser og netværk
	
	Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.
		Forespurgt om 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 og opfølgning på logs.
		
		Forespurgt om logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, har været konfigureret og aktiveret på erklæringstidspunktet.
		
		Forespurgt om opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning.
		
		Inspiceret ud fra en tilfældigt udvalgt dags logning, at logfiler har det forventede indhold i forhold til opsætning, samt inspiceret dokumentation for den foretagne opfølgning og håndtering af evt. sikkerhedshændelser, aktiviteter udført af systemadministratorer og andre med særlige rettigheder mv.
			Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Nr.	Databehandlerens kontrolaktivitet	Baker Tillys 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.	Forespurgt om 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 for en tilfældigt udvalgt udviklings- henholdsvis testdatabase, at personoplysninger heri er pseudonymiseret eller anonymiseret.	Ingen anmærkninger.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Forespurgt om der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførsel af sårbarheds-scanninger og penetrationstests. Inspiceret dokumentation for de seneste tests af de etablerede tekniske foranstaltninger. Forespurgt om evt. afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret samt meddelt de dataansvarlige i behørigt omfang.	Ingen anmærkninger.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Forespurgt om der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerheds-patches. Inspiceret ved udtræk eller opslag af tekniske sikkerhedsparametre og -opsætninger, for en enkelt af hver type systemer, databaser og netværk der anvendes, at disse er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Nr.	Databehandlerens kontrolaktivitet	Baker Tillys udførte test	Resultat af test
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til person-oplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Forespurgt om der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Inspiceret for en enkelt medarbejder for hver gruppe af medarbejdere at adgange til systemer og databaser, er godkendt, og at der er et arbejdsbetinget behov. Inspiceret for en enkelt tilfældig udvalgt fratrådt medarbejder, at dennes adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Inspiceret dokumentation for at periodisk vurdering og godkendelse af tildelte brugeradgange er udført efter planen.	Ingen anmærkninger.
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor autentifikation.	Forespurgt om der foreligger formaliserede procedurer, der sikrer, at to-faktor autentifikation anvendes ved behandling af personoplysninger, der medfører højrisiko for de registrerede. Observeret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører høj-risiko for de registrerede, alene kan ske ved anvendelse af to-faktor autentifikation.	Ingen anmærkninger
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.	Forespurgt om der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Observeret for tilfældigt udvalgte lokaler og data-centre, hvori der opbevares og behandles personoplysninger, at det er sandsynligt at kun autoriserede personer har haft fysisk adgang hertil på erklæringstidspunktet.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Kontrolmål C:

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

Nr.	Databehandlerens kontrolaktivitet	Baker Tillys udførte test	Resultat af test
C.1	Databehandlerens ledelse har godkendt en skriftlig in-formationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Forespurgt om der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Forespørg om hvordan informationssikkerheds-politikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Ingen anmærkninger.
C.2	Databehandlerens ledelse har sikret, at informa-tionssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Inspiceret ved en repræsentativ databehandleraftale, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Ingen anmærkninger.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Forespurgt om der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Inspiceret ved en tilfældigt udvalgt nyansat medarbejder, at der er dokumentation for efterprøvning.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Nr.	Databehandlerens kontrolaktivitet	Baker Tillys udførte test	Resultat af test
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	Inspiceret for en tilfældigt udvalgt nyansat medarbejder på erklæringstidspunktet, at den pågældende medarbejder har underskrevet en fortrolighedsaftale og er blevet introduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling, samt anden relevant information	Ingen anmærkninger.
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Forespurgt om der foreligger procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages. Inspiceret for en tilfældigt udvalgt fratrådt medarbejder på erklæringstidspunktet, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.	Ingen anmærkninger.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	Forespurgt om der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Inspiceret for en tilfældigt udvalgt fratrådt medarbejder på erklæringstidspunktet, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt.	Ingen anmærkninger.
C.7	Der gennemføres løbende awarenesstræning af data-behandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Forespurgt om databehandleren udbyder awarenesstræning 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 awarenesstræning.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

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	Baker Tillys udførte test	Resultat af test
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overens-stemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Forespurgt om der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Forespurgt om hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget. Inspiceret oversigt over skriftlige procedurer og vurdereret om denne forekommer opdateret og tilstrækkelig i forhold til aftalte opbevaring og sletning af personoplysninger.	Ingen anmærkninger.
D.2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: • Alle personoplysninger slettes som standard efter 30 dage. • Sletning af personoplysninger ved data-behandleraftalens ophør.	Forespurgt om de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Inspiceret for en tilfældigt udvalgt databehandling fra databehandlerens oversigt over behandlings-aktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder og sletterutiner.	Ingen anmærkninger.
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning	Forespurgt om der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Inspiceret for en tilfældigt udvalgt ophørte databehandling på erklæringstidspunktet, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Kontrolmål E:

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

Nr.	Databehandlerens kontrolaktivitet	Baker Tillys 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 en gang årligt – vurdering af, om procedurerne skal opdateres.	Forespurgt om der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Forespurgt om hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget. Inspiceret for en tilfældigt udvalgt databehandling fra databehandlerens oversigt over behandlings-aktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Ingen anmærkninger.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Forespurgt om databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Inspiceret for en tilfældigt udvalgt databehandling fra databehandlerens oversigt over behandlings-aktiviteter, 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 anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Kontrolmål F:

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

Nr.	Databehandlerens kontrolaktivitet	Baker Tillys 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 en gang årligt – vurdering af, om procedurerne skal opdateres.	Forespurgt om der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Forespurgt om hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget. Inspiceret oversigt over skriftlige procedurer og vurdereret om denne forekommer opdateret og tilstrækkelig i forhold til anvendelse af underdatabehandlere.	Ingen anmærkninger.
F.2	Databehandleren anvender alene underdata-behandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Forespurgt om databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Inspiceret for en tilfældigt udvalgt underdatabehandler fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige (specifikt eller indirekte).	Ingen anmærkninger.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdata-behandlere er dette godkendt af den dataansvar-lige.	Forespurgt om der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne på erklæringstidspunktet.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Nr.	Databehandlerens kontrolaktivitet	Baker Tillys udførte test	Resultat af test
F.4	Databehandleren har pålagt underdata-behandleren de samme databeskyttelses-forpligtelser som dem, der er forudsat i databe-handleraftalen el.lign. med den dataansvarlige.	Forespurgt om der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Inspiceret for en tilfældigt udvalgt underdatabehandleraftale, at denne indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen anmærkninger.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen	Forespurgt om databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret for en enkelt underdatabehandler at oversigten indeholder de krævede oplysninger.	Ingen anmærkninger.
F.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Forespurgt om der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Inspiceret dokumentation for, at der er foretaget en risikovurdering af en tilfældigt udvalgt underdatabehandler og den aktuelle behandlingsaktivitet hos denne, samt at de er foretaget planlagt opfølgning i overensstemmelse med risikovurderingen.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

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	Baker Tillys 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 en gang årligt – vurdering af, om procedurerne skal opdateres.	Forespurgt om der foreligger formaliserede procedurer, der sikrer, at personoplysninger alene overføres til tredjelande eller internationale organisationer i henhold til aftale med den data-ansvarlige på baggrund af et gyldigt overførsels-grundlag. Forespurgt om hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget. Inspiceret oversigt over skriftlige procedurer og vurdereret om denne forekommer opdateret og tilstrækkelig i forhold til overførsel af personoplysninger.	Ingen anmærkninger.
G.2	Databehandleren må kun overføre person-oplysninger til tredjelande eller internationale organisationer efter instruks fra den data-ansvarlige.	Forespurgt om databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer. Inspiceret for en tilfældigt udvalgt dataoverførsel fra databehandlerens oversigt over overførsler, at der er dokumentation for, at overførslen er aftalt med den dataansvarlige i databehandleraftalen eller udført efter modtaget instruks fra den dataansvarlige.	Ingen anmærkninger.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Forespurgt om der foreligger formaliserede procedurer for sikring af et gyldigt overførselsgrund-lag. Forespurgt om hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget. Inspiceret for en tilfældigt udvalgt 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 anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

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	Baker Tillys 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 en gang årligt – vurdering af, om procedurerne skal opdateres.	Forespurgt om der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Forespurgt om hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget. Inspiceret oversigt over skriftlige procedurer og vurdereret om denne forekommer opdateret og tilstrækkelig i forhold til bistand til den dataansvarlige.	Ingen anmærkninger.
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.	Forespurgt om 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. Vurderet om det er sandsynligt, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Kontrolmål I:

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

Nr.	Databehandlerens kontrolaktivitet	Baker Tillys 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 en gang årligt – vurdering af, om procedurerne skal opdateres.	Forespurgt om der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikker-heden. Forespurgt om hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget. Inspiceret oversigt over skriftlige procedurer og vurdereret om denne forekommer opdateret og tilstrækkelig i forhold til håndtering af sikkerhedsbrud.	Ingen anmærkninger.
I.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på person-datasikkerheden: • Awareness hos medarbejdere • Overvågning af netværkstrafik • Opfølgning på logning af tilgang til personoplysninger	Forespurgt om databehandler udbyder awarenesstræning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikker-heden. Inspiceret dokumentation for, at netværkstrafik overvåges, samt at der sker opfølgning på anormaliteter, overvågningsalarmer, overførsel af store filer mv. Forespurgt om hvordan det sikres at der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang.	Ingen anmærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf (fortsat)

Kontrolmål I:

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

Nr.	Databehandlerens kontrolaktivitet	Baker Tillys udførte test	Resultat af test
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den data-ansvarlige 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.	Forespurgt om databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Forespurgt underdatabehandlerne, om de har konstateret nogen brud på persondatasikkerheden på erklæringstidspunktet. Forespurgt om databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser. Forespurgt om samtlige registrerede brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødig forsinkelse og senest 24 timer efter, at databehandleren er blevet opmærksom på brud på persondatasikker-heden.	Der har ikke været konstateret brud på persondatasikkerheden. Ingen øvrige anmærkninger.
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på person-datasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Forespurgt om de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for: • Beskrivelse af karakteren af bruddet på persondata-sikkerheden • Beskrivelse af sandsynlige konsekvenser af bruddet på persondata-sikkerheden • Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. Vurderet om det er sandsynligt, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.	Ingen anmærkninger.

Baker Tilly GDPR ansvarlig partner

Now, for tomorrow

Baker Tilly Denmark
Godkendt Revisionspartnerselskab

København
Poul Bundgaards Vej 1, 1. sal
2500 Valby
T: +45 3345 1000

Sorø
Storgade 24A
4180 Sorø
T: +45 3345 1000

Odense
Hjallesevej 126
5230 Odense M
T: +45 6613 0730

bakertilly.dk

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

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

Michael Brink Larsen
BAKER TILLY DENMARK GODKENDT REVISIONSPARTNERSELSKAB CVR: 35257691
Statsautoriseret revisor
På vegne af: Baker Tilly Denmark Godkendt Revisionsp…
Serienummer: f0c28aad-9c66-4dd4-9020-15bb8d0b4494
IP: 91.221.xxx.xxx
2024-10-31 10:00:36 UTC

Ole Knudsen
Adm. direktør
På vegne af: G4S Security Services A/S
Serienummer: 30c20b7a-a156-422e-9d82-ad3b419cc607
IP: 87.49.xxx.xxx
2024-10-31 10:01:36 UTC