AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 16. MAJ 2024 TIL 15. MAJ 2025 OM BESKRIVELSEN AF COMPAYAS SMS-SYSTEMER (CPSMS.DK, PROSMS.SE/SMS.DK OG SMS1919.DK) OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER, DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

compaya© MOBILE SOLUTIONS

BDO

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 16. MAJ 2024 TIL 15. MAJ 2025 OM BESKRIVELSEN AF COMPAYAS SMS-SYSTEMER OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER, DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

Til: Ledelsen i Compaya A/S
Compaya A/S' kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af Compaya A/S (databehandleren) for hele perioden fra 16. maj 2024 til 15. maj 2025 udarbejdede beskrivelse i sektion 3 af SMS-systemer og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelse af personoplysninger i henhold til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) og lov om supplerende bestemmelser til databeskyttelsesforordningen (databeskyttelsesloven), og om udformningen og den operationelle effektivitet af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Databehandlerens ansvar

Databehandleren er ansvarlig for udarbejdelse af udtalelsen i sektion 2 og den medfølgende beskrivelse, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå udtalelsen og beskrivelsen er præsenteret. Databehandleren er endvidere ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, ligesom databehandleren er ansvarlig for at anføre kontrolmålene samt udforme, implementere og effektivt udføre 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.

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

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om databehandlerens beskrivelse samt om udformningen og den operationelle effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og den operationelle effektivitet af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse samt for kontrollernes udformning og operationelle effektivitet. De valgte handlinger afhænger af databehandlerens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af den operationelle effektivitet af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte kontrolmål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i sektion 2.

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

Databehandlerens beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved anvendelsen af SMS-systemer, som hver enkelt dataansvarlig måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. Herudover er fremskrivningen af enhver vurdering af den operationelle effektivitet af kontroller 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 databehandlerens udtalelse i sektion 2. Det er vores opfattelse:

a. at beskrivelsen af SMS-systemer og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelse af personoplysninger i henhold til databeskyttelsesforordningen og databeskyttelsesloven, således som de var udformet og implementeret i hele perioden 16. maj 2024 til 15. maj 2025, i alle væsentlige henseender er retvisende, og

b. at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden 16. maj 2024 til 15. maj 2025, og

c. at de testede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som var de, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden 16. maj 2024 til 15. maj 2025.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, og resultater af disse tests fremgår i sektion 4.

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt dataansvarlige, der har anvendt databehandlerens SMS-systemer, og som har en tilstrækkelig forståelse til at vurdere den sammen med anden information, herunder de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

København, den 3. juli 2025

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

Mikkel Jon Larssen
Partner, chef for Risk Assurance, CISA, CRISC

2. COMPAYA A/S' UDTALELSE

Compaya A/S varetager behandling af personoplysninger i forbindelse med SMS-systemer for vores kunder, der er dataansvarlige i henhold til Europa-Parlaments og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) og lov om supplerende bestemmelser til databeskyttelsesforordningen (databeskyttelsesloven).

Medfølgende beskrivelse er udarbejdet til brug for de dataansvarlige, der har anvendt SMS-systemer, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

Compaya A/S anvender underdatabehandlere. Disse underdatabehandleres relevante kontrolmål og tilknyttede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller indgår ikke i den medfølgende beskrivelse.

Compaya A/S bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af SMS-systemer og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller i hele perioden 16. maj 2024 til 15. maj 2025. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for SMS-systemer, og hvordan de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller 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 forretningsgange der er anvendt til at behandle personoplysninger og, om nødvendigt, at korrigere og slette personoplysninger samt at 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 til 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.
    - De kontroller, som vi med henvisning til afgrænsningen af SMS-systemer har forudsat ville være udformet og implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå kontrolmålene, er identificeret i beskrivelsen.
    - De andre aspekter ved kontrolmiljøet, risikovurderingsprocessen, informationssystemerne og kommunikationen, kontrolaktiviteterne og overvågningskontrollerne, som har været relevante for behandlingen af personoplysninger.

2. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af SMS-systemer og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller under hensyntagen til, at denne beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved SMS-systemer, som den enkelte dataansvarlige måtte anse vigtig efter deres særlige forhold.

Compaya A/S bekræfter, at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden 16. maj 2024 til 15. maj 2025. Kriterierne anvendt for at give denne udtalelse var, at:

1. De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret.

2. 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.

3. Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse, i hele perioden 16. maj 2024 til 15. maj 2025.

Compaya A/S bekræfter, at der er implementeret og opretholdt passende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

København, den 3. juli 2025

Compaya A/S

Martin Saldern Schrøder
Direktør/Partner

3. COMPAYA A/S' BESKRIVELSE AF SMS-SYSTEMER

COMPAYA A/S

Compaya A/S (Compaya) er en danskejet virksomhed, der udvikler og driver online-tjenesterne CPSMS.dk, ProSMS.se/SMS.dk og SMS1919 til virksomheder, foreninger, offentlige institutioner mv. Compaya har kontor i København.

Compaya's ca. 9 medarbejdere er specialiserede inden for salg og marketing, systemudvikling, serverdrift, support og informationssikkerhed, og er organiseret i en salgsafdeling og en udviklingsafdeling.

IT-sikkerhedsansvarlig styrer Compaya's persondatasikkerhed i forhold til den behandling, som Compaya varetager på vegne af sine kunder, herunder indgåelse af databehandleraftaler, besvarelse af henvendelser fra den dataansvarlige, underretning om brud på persondatasikkerheden, efterlevelse af interne politikker og procedurer og lignende.

SMS-SYSTEMERNE OG BEHANDLING AF PERSONOPLYSNINGER

Compaya leverer SMS-systemerne som Software-as-a-Service (SaaS) løsninger. Kunderne skal for at benytte SMS-systemerne acceptere de handelsvilkår, der fremgår af de respektive systemers hjemmesider. I nogle tilfælde ønsker kunderne en specifik hovedaftale, og en sådan udarbejdes efter forlangende. Vi opfordrer via hjemmesiderne og i SMS-systemerne kunderne til, at der skal indgås en databehandleraftale, og danner denne elektronisk eller fremsender efter behov i givet fald Compaya's standard databehandleraftale tilpasset den enkelte kunde.

SMS-systemerne udvikles på kontoret i København, men afvikles fra eksterne hostingcentre, som dermed er underdatabehandlere. Compaya har indgået databehandleraftale med disse underdatabehandlere.

I forbindelse med dataansvarliges brug af SMS-systemerne indsamler og behandler Compaya personoplysninger om den dataansvarlige. Disse data omfatter firmanavn, adresse, navn, e-mail, telefonnummer, CVR-nummer og evt. EAN-nummer samt log over aktivitet ved brug af SMS-systemerne. Der er alene tale om almindelige personoplysninger.

I SMS-systemerne angiver dataansvarliges brugere personoplysninger om modtagere af SMS-beskeder. Det drejer sig specifikt om mobilnummer og evt. navn. Dataansvarlige kan endvidere have angivet personoplysninger i selve SMS-beskedens tekstfelt.

Som udgangspunkt udfører Compaya databehandling i form af opbevaring og transmittering af de SMS-beskeder, som dataansvarlige har indlagt i SMS-systemerne. Der gemmes en log over de afsendte SMS-beskeder, og de ansatte i Compaya har via denne log adgang til oplysningerne i disse SMS-beskeder via de brugerroller, der er opsat som systemadgange. Denne adgang benyttes i forbindelse med afhjælpning af problemer for dataansvarlige.

STYRING AF PERSONDATASIKKERHED

Compaya har opstillet krav til etablering, implementering, vedligeholdelse og løbende forbedring af et ledelsessystem for persondatasikkerhed, der sikrer opfyldelse af indgåede aftaler med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

De tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller til beskyttelse af personoplysninger er udformet i henhold til risikovurderinger og implementeres for at sikre fortrolighed, integritet og tilgængelighed samt overholdelse af den gældende databeskyttelseslovgivning. Sikkerhedsforanstaltninger og kontroller er i videst muligt omfang automatiserede og teknisk understøttet af it-systemer.

Styringen af persondatasikkerheden samt de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller er struktureret i følgende hovedområder, for hvilke der er defineret kontrolmål og kontrol- aktiviteter:

ARTIKEL	OMRÅDE
Artikel 28, stk. 1	Databehandlerens garantier
Artikel 28, stk. 3	Databehandleraftale
Artikel 28, stk. 3, litra a og h, og stk. 10 Artikel 29 Artikel 32, stk. 4	Instruks for behandling af personoplysninger
Artikel 28, stk. 2 og 4	Underdatabehandlere
Artikel 28. stk. 3, litra b	Fortrolighed og lovbestemt tavshedspligt
Artikel 28, stk. 3, litra c	Tekniske og organisatoriske sikkerhedsforanstaltninger
Artikel 25	Databeskyttelse gennem design og standardindstillinger.
Artikel 28, stk. 3, litra g	Sletning og tilbagelevering af personoplysninger
Artikel 28, stk. 3, litra e, f og h	Bistand til den dataansvarlige
Artikel 30, stk. 2, 3 og 4	Fortegnelse over kategorier af behandlingsaktiviteter
Artikel 33, stk. 2	Underretning om brud på persondatasikkerheden.

RISIKOVURDERING

Ledelsen er ansvarlig for, at der iværksættes alle de initiativer, der imødegår det trusselsbillede, som Compaya til enhver tid står over for, således at indførte sikkerhedsforanstaltninger og kontroller er passende, og risikoen for brud på persondatasikkerheden reduceres til et passende niveau.

Der foretages en løbende vurdering af, hvilket sikkerhedsniveau der er passende. I vurderingen tages der hensyn til risici i forhold til personoplysningers hændelige eller ulovlige tilintetgørelse, tab eller ændring, eller uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Som grundlag for ajourføring af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller udføres der en gang årligt en risikovurdering. Risikovurderingen belyser sandsynligheden for og konsekvenserne af hændelser, der kan true persondatasikkerheden og dermed fysiske personers rettigheder og frihedsrettigheder, herunder tilfældige, forsætlige og uforsætlige hændelser. Risikovurderingen tager hensyn til det aktuelle tekniske niveau og implementeringsomkostningerne. Som led i risikovurderingen er udført en konsekvensanalyse (DPIA) for SMS-systemerne. Compaya har endvidere benyttet modellen Risknon fra Risikoanalyser.dk til sin risikoanalyse.

TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER

De tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller vedrører alle processer og systemer, som behandler personoplysninger på vegne af den dataansvarlige. De i kontrolskemaet anførte kontrolmål og kontrolaktiviteter er en integreret del af den efterfølgende beskrivelse.

Databehandlerens garantier

Compaya har indført politikker og procedurer, der sikrer, at Compaya kan stille tilstrækkelige garantier til at gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder. Compaya har etableret en organisering af persondatasikkerheden samt udarbejdet og implementeret en af ledelsen godkendt informationssikkerhedspolitik, der løbende gennemgås og opdateres.
Der forefindes procedurer for rekruttering og fratrædelse af medarbejdere samt retningslinjer for uddannelse og instruktion af medarbejdere, der behandler personoplysninger, herunder gennemførelse af awareness og oplysningskampagner.

Databehandleraftaler

Compaya har indført procedure for indgåelse af databehandlingsaftaler, der angiver betingelserne for behandling af personoplysninger på vegne af den dataansvarlige. Compaya anvender Datatilsynets skabelon for databehandleraftaler i overensstemmelse med de tjenester, der leveres, herunder information om brugen af underdatabehandlere. Databehandleraftalerne underskrives af begge parter og opbevares elektronisk.

Compaya udfører som databehandler kun behandling af personoplysninger efter dokumenteret instruks fra den dataansvarlige, enten i databehandleraftalen eller i nogle tilfælde efter en af den dataansvarlige udarbejdet separat instruks.

Som databehandler underretter Compaya omgående den dataansvarlige, hvis en instruks efter Compaya's mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

Underdatabehandlere

Databehandleren har den dataansvarliges generelle godkendelse til at gøre brug af underdatabehandlere. Databehandleren skal dog indhente godkendelse hos den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre underdatabehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.

Compaya benytter alene underdatabehandlere til serverhosting i forbindelse med drift af SMS-systemerne.

Underdatabehandler skal hvert år, typisk i marts måned, sende en erklæring for det foregående år fra et godkendt revisionsselskab angående underdatabehandlers implementering af egne retningslinjer samt tilstrækkeligheden heraf.

Fortrolighed og lovbestemt tavshedspligt

Som databehandler sikrer Compaya, at kun de personer, der aktuelt er autoriseret hertil, har adgang til de personoplysninger, der behandles på vegne af den dataansvarlige. Adgangen til oplysningerne lukkes derfor straks ned, hvis autorisationen fratages eller udløber.

Der må alene autoriseres personer, for hvem det er nødvendigt at have adgang til personoplysningerne for at kunne opfylde databehandlerens forpligtelser overfor den dataansvarlige.

Som databehandler sikrer Compaya, at de personer, der er autoriseret til at behandle personoplysninger på vegne af den dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

Som databehandler kan Compaya efter anmodning fra den dataansvarlige påvise, at de relevante medarbejdere er underlagt ovennævnte tavshedspligt.

Tekniske og organisatoriske sikkerhedsforanstaltninger

Risikovurdering
Compaya har gennemført de tekniske og organisatoriske sikkerhedsforanstaltninger på baggrund af en vurdering af risici i forhold til fortrolighed, integritet og tilgængelighed. Der henvises til særskilt afsnit herom.

Beredskabsplaner
Compaya har etableret beredskabsplaner, således at Compaya rettidigt kan genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af fysiske eller tekniske hændelser. Compaya har etableret et kriseberedskab, der træder i kraft i disse tilfælde. Organisering af kriseberedskabsgruppe er etableret, og der er indført retningslinjer for aktivering af kriseberedskabet.

Compaya har udformet detaljerede beredskabsplaner og planer for retablering af systemer og data. Planerne er tilgængelige via Dropbox. Planerne afprøves og revideres løbende i forbindelse med ændringer i systemer mv.

Opbevaring af personoplysninger
Compaya har indført procedurer, der sikrer, at opbevaring af personoplysninger alene foretages i overensstemmelse med Compaya's persondatapolitik. Adgang til personoplysninger tildeles på baggrund af arbejdsbetinget behov/need-to-know principper.

Fysisk adgangskontrol
Compaya har indført procedurer, der sikrer, at lokaler er beskyttet mod uautoriseret adgang. Compaya har ikke sikrede lokaler (serverrum og lign.), og har derfor ikke adgangskontrol med nøglekort eller lign. Kunder, leverandører og andre besøgende ledsages. Uden for normal arbejdstid kræves kode til alarmsystem for at komme ind på adressen.

Compaya benytter hosting-leverandører til alle servere. Compaya har ikke adgang til hosting-leverandørernes faciliteter. Kun autoriserede medarbejdere hos hosting-leverandørerne har adgang til disse.

Logisk adgangssikkerhed
Compaya har etableret kontroller, der sikrer, at adgang til systemer og data er beskyttet mod uautoriseret adgang til personoplysninger. En bruger oprettes med unik brugeridentifikation og password, og bruger- identifikation anvendes ved tildeling af adgang til ressourcer og systemer. Al tildeling af rettigheder i systemer sker ud fra et arbejdsbetinget behov. Der foretages mindst en gang årligt en evaluering af brugernes fortsatte arbejdsbetingede behov for adgang, herunder aktualitet og korrekthed for tildelte brugerrettigheder. Procedurer og kontroller understøtter processen for oprettelse, ændring og nedlæggelse af brugere og tildeling af rettigheder samt gennemgang heraf.

Udformning af krav til blandt andet længde og kompleksitet af password samt lukning af brugerkonto efter forgæves adgangsforsøg følger best practice for en sikker logisk adgangskontrol. Der er udformet tekniske foranstaltninger, der understøtter disse krav.

Fjernarbejdspladser og fjernadgang til systemer og data
Compaya har implementeret procedurer, der sikrer, at adgang fra arbejdspladser uden for Compaya's lokaler og fjernadgang til servere og data sker via VPN-forbindelser. Compaya har implementeret procedurer der sikrer, at eksterne kommunikationsforbindelser er sikret med kryptering.

Netværkssikkerhed
Compaya har indført procedurer, der sikrer netværk i forhold til anvendelse og sikkerhed. Compaya's netværk til drift befinder sig hos team.blue Denmark A/S (Zitcom/Curanet/Wannafind) samt hos Rackhosting ApS og er adskilt fra Compaya's kontornetværk. Adgang mellem netværkene begrænses så vidt muligt, og adgangen styres jf. ovenstående. I Compaya's lokaler i Palægade findes alene netværksudstyr til kontornetværket, som er opdelt i VLAN's.

Kontornetværket hos Compaya på adressen i Palægade 4 er beskyttet af den firewall, der ligger i vores router, hvor der overordnet er lukket for alt indgående og åbent for alt udgående trafik. Samtlige PC'er og bærbare er desuden beskyttet af software firewall i Bitdefender Endpoint Security.

Systemerne CPSMS og SMS1919 befinder sig hos hosting leverandør team.blue og er beskyttet af den firewall som team.blue drifter. Systemet PROSMS befinder sig hos hosting leverandør Rackhosting og er beskyttet af den hardware firewall som Rackhosting drifter. Hver server er desuden beskyttet af en software firewall, som Compaya administrerer.

Antivirusprogram og systemopdateringer
Compaya har indført procedurer, der sikrer, at enheder med adgang til netværk og applikationer er beskyttet mod virus og malware. Der sker en løbende opdatering og tilpasning af antivirusprogrammer og andre beskyttelsessystemer i forhold til det aktuelle trusselsniveau.

Compaya har indført procedurer, der sikrer, at systemsoftware opdateres løbende efter leverandørernes forskrifter og anbefalinger. Procedurer for Patch Management omfatter operativsystemer, kritiske services og relevant software installeret på servere og arbejdsstationer.

Sikkerhedskopiering og retablering af data
Compaya har indført procedurer, der sikrer, at systemer og data sikkerhedskopieres for at imødegå tab af data eller tab af tilgængelighed ved nedbrud. Sikkerhedskopier opbevares på alternativ lokation. Der udføres løbende, dog mindst en gang om året, en restore-test af backup.

Logning af anvendelse af personoplysninger
Compaya har indført procedurer, der sikrer, at logning er opsat i henhold til lovgivningens krav og forretningsmæssige behov, baseret på en risikovurdering af systemer og det aktuelle trusselsniveau. Omfang og kvalitet af logdata er tilstrækkelig til at identificere og påvise eventuelt misbrug af systemer eller data, og logdata gennemgås løbende for anvendelighed og unormal adfærd. Logdata er sikret.

Overvågning
Compaya har indført procedurer, der sikrer, at der sker løbende overvågning af systemer og indførte tekniske sikkerhedsforanstaltninger.

Bortskaffelse af it-udstyr
Lagringsmedier, der skal destrueres, kan afleveres til IT-sikkerhedsmedarbejder eller til IT-udviklingschef, der skal sørge for en effektiv og permanent destruktion af mediet eller data derpå.

Databeskyttelse gennem design og standarder

Compaya har indført politikker og procedurer for udvikling og vedligeholdelse af SMS-systemerne, der sikrer en styret ændringsproces. Der anvendes en Change Management procedure til styring af udviklings- og ændringsopgaver, og enhver opgave følger en ensartet proces.

Udviklings-, test- og produktionsmiljø er adskilte, og enhver udviklings- og ændringsopgave gennemløber et testforløb. Der er indført procedurer for versionskontrol, logning og sikkerhedskopiering, således at det er muligt at geninstallere tidligere versioner.

Sletning og tilbagelevering af personoplysninger
Compaya har indført politikker og procedurer, der sikrer, at personoplysninger slettes i henhold til instruks fra den dataansvarlige, når behandlingen af personoplysninger ophører ved udløb af kontrakten med den dataansvarlige.

Bistand til den dataansvarlige

Compaya har indført politikker og procedurer, der sikrer, at Compaya kan bistå den dataansvarlige med at opfylde dennes forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder.

Compaya har indført politikker og procedurer, der sikrer, at Compaya kan bistå den dataansvarlige med at sikre overholdelse af forpligtelserne i artikel 32 om behandlingssikkerhed, artikel 33 om anmeldelse og underretning af brud på persondatasikkerheden samt artikel 34 – 36 om konsekvensanalyser.

Compaya har indført politikker og procedurer, der sikrer, at Compaya kan stille alle oplysninger, der er nødvendige for at påvise overholdelse af kravene til databehandlere, til rådighed for den dataansvarlige.
Compaya giver desuden mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller andre, som er bemyndiget hertil af den dataansvarlige.

Fortegnelse over kategorier af behandlingsaktiviteter

Compaya har indført politikker og procedurer, der sikrer, at der føres en fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige. Fortegnelsen opdateres regelmæssigt og kontrolleres under den årlige gennemgang af politikker og procedurer mv. Fortegnelsen opbevares elektronisk og kan stilles til rådighed for tilsynsmyndigheden efter anmodning.

Underretning om brud på persondatasikkerheden

Compaya har indført politikker og procedurer, der sikrer, at brud på persondatasikkerheden registreres med detaljeret information om hændelsen, og at der sker underretning af den dataansvarlige uden unødig forsinkelse, efter at Compaya er blevet opmærksom på, at der er sket brud på persondatasikkerheden.

De registrerede informationer gør den dataansvarlige i stand til at foretage en vurdering af, om bruddet på persondatasikkerheden skal anmeldes til tilsynsmyndigheden, og om de registrerede skal underrettes.

KOMPLEMENTERENDE KONTROLLER HOS DE DATAANSVARLIGE

Som et 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.

Den dataansvarlige har bl.a. følgende forpligtelser:

- Sikring af, at instruksen i den indgåede databehandleraftale er lovlig set i forhold til den til enhver tid gældende persondataretlige regulering.
- Sikring af, at instruksen i den indgåede databehandleraftale er hensigtsmæssig set i forhold til hovedydelsen.
- Ansvaret for at sikre, at administratorernes brug af SMS-systemerne og den behandling af personoplysninger, der foretages i systemerne, sker i overensstemmelse med databeskyttelseslovgivningen.
- Sikring af, at eventuelle særlige krav til sikkerhedsforanstaltninger hos den dataansvarlige er beskrevet i den indgåede databehandleraftale.
- Sikring af, at den dataansvarliges brugere i SMS-systemerne er ajourførte.

4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST

Formål og omfang

BDO har udført sit arbejde i overensstemmelse med ISAE 3000 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger.

BDO har udført handlinger for at opnå bevis for oplysningerne i Compaya A/S beskrivelse af SMS-systemer samt for udformningen af de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. De valgte handlinger afhænger af BDO's vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller fungerer effektivt.

BDO's test af udformningen af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller samt implementeringen heraf har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af Compaya A/S, og som fremgår af efterfølgende kontrolskema.

I kontrolskemaet har BDO beskrevet de udførte test, der blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og at de tilhørende kontroller var hensigtsmæssigt udformet og fungerede effektivt fra 16. maj 2024 til 15. maj 2025.

Udførte testhandlinger

Test af udformningen af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller samt implementeringen heraf er udført ved forespørgsel, inspektion, observation og genudførsel.

Type	Beskrivelse
Forespørgsel	Forespørgsler hos passende personale er udført for alle væsentlige kontrolaktiviteter. Forespørgslerne blev udført for blandt andet at opnå viden og yderligere oplysninger om indførte politikker og procedurer, herunder hvordan kontrolaktiviteterne udføres, samt at få bekræftet beviser for politikker, procedurer og kontroller.
Inspektion	Dokumenter og rapporter, der indeholder angivelse om udførelse af kontrollen, er gennemlæste med det formål at vurdere udformningen og overvågningen af de specifikke kontroller, herunder om kontrollerne er udformede således, at de kan forventes at blive effektive, hvis de implementeres, og om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Test af væsentlige systemopsætninger af tekniske platforme, databaser og netværksudstyr er udført for at påse, om kontroller er implementeret, herunder eksempelvis vurdering af logning, sikkerhedskopiering, patch management, autorisationer og adgangskontroller, datatransmission samt besigtigelse af udstyr og lokaliteter.
Observation	Anvendelsen og eksistensen af specifikke kontroller er observeret, herunder test for at påse, at kontrollen er implementeret.
Genudførelse	Kontroller er genudført for at verificere, at kontrollen fungerer som forudsat.

For de ydelser, som Rackhosting ApS leverer inden for hostingydelser, har vi modtaget en ISAE 3000-erklæring om informationssikkerhed og foranstaltninger, samt ISAE 3402-erklæring vedr. generelle it-kontroller i forbindelse med driftsydelser til kunder, begge for perioden 1. maj 2023 til 30. april 2024 i henhold til databehandleraftale.

For de ydelser, som team.blue Denmark A/S (Zitcom/Curanet/Wannafind) leverer inden for hostingydelser, har vi modtaget en ISAE 3402 erklæring om generelle it-kontroller relateret til hostingydelser for perioden 1. januar til 31. december 2024.
For de ydelser, som Curanet A/S leverer inden for hostingydelser, har vi modtaget en ISAE 3402 erklæring om generelle it-kontroller relateret til hostingydelser for perioden 1. januar til 31. december 2024.

Disse underdatabehandlers relevante kontrolmål og tilknyttede kontroller indgår ikke i Compaya A/S' beskrivelse af SMS-systemer og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos Compaya A/S, der sikrer udførelsen af et behørigt tilsyn med underdatabehandlerens opfyldelse af den mellem underdatabehandleren og databehandleren indgåede databehandleraftale og opfyldelse af databeskyttelsesforordningen og databeskyttelsesloven.

Resultat af test

Resultatet af de udførte test af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller angiver, om den beskrevne test har givet anledning til at konstatere afvigelser.

En afvigelse foreligger, når:

- Tekniske eller organisatoriske sikkerhedsforanstaltninger eller øvrige kontroller mangler at blive udformet og implementeret for at kunne opfylde et kontrolmål.
- Tekniske eller organisatoriske sikkerhedsforanstaltninger eller øvrige kontroller, der knytter sig til et kontrolmål, ikke er hensigtsmæssigt udformet, implementeret eller ikke er effektiv.

Artikel 28, stk. 1: Databehandlerens garantier		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Politikker for informationssikkerhed og gennemgang af politikker for informationssikkerhed ▶ Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. ▶ Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt. Vi har inspiceret, at procedurer er opdateret og godkendt i erklæringsperioden.	Ingen afvigelser konstateret.
Informationsikkerhedspolitikker i overensstemmelse med databehandleraftaler ▶ Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Vi har stikprøvevis inspiceret, at kravene i indgåede databehandleaftaler ikke er modstridende med informationssikkerhedspolitikken.	Ingen afvigelser konstateret.
Rekruttering af medarbejdere – Screening ▶ Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: ○ Referencer fra tidligere ansættelser ○ CV ○ Evt. Eksamensbeviser	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Vi har konstateret, at der er etableret en procedure for screening. Vi har ikke kunnet udtale os om kontrollens implementering og effektivitet, da der ikke i erklæringsperioden har været tiltrædelser. Ingen afvigelser konstateret.

Artikel 28, stk. 1: Databehandlerens garantier		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Fratrædelse af medarbejdere - inddragelse af adgangsrettigheder og aktiver ▶ Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages.	Vi har konstateret, at der er etableret en procedure for inddragelse af adgangsrettigheder. Vi har ikke kunnet udtale os om kontrollens implementering og effektivitet, da der ikke i erklæringsperioden har været fratrædelser. Ingen afvigelser konstateret.
Fratrædelse af medarbejdere - oplysning om fortrolighed og tavshedspligt ▶ 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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har udarbejdet en proces for oplysning om fortrolighed og tavshedspligt.	Vi har konstateret, at der er etableret en procedure for oplysning om fortrolighed og tavshedspligt. Vi har ikke kunnet udtale os om kontrollens implementering og effektivitet, da der ikke i erklæringsperioden har været fratrædelser. Ingen afvigelser konstateret.
Awareness, uddannelse og træning vedrørende informationssikkerhed ▶ Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Vi har inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, artikel 29, artikel 30, stk. 2, 3 og 4 og artikel 32, stk. 4: Databehandleraftale og behandling af personoplysninger på vegne af dataansvarliges instruks		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Procedure for behandling af personoplysninger ▶ 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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger en formaliseret procedure, der skal sikre, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har inspiceret, at proceduren indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Vi har inspiceret, at proceduren er opdateret og ledelsesgodkendt i erklæringsperioden.	Ingen afvigelser konstateret.
Efterlevelse af instruks for behandling af personoplysninger ▶ Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har stikprøvevis inspiceret indgåede databehandleraftaler med dataansvarlige og observeret, at aftalerne indeholder instrukser fra dataansvarlige. Vi har inspiceret databehandlerens fortegnelse over behandlingsaktiviteter og stikprøvevis inspiceret, at behandlingerne foregår i overensstemmelse med instruks fra dataansvarlig.	Ingen afvigelser konstateret.
Underretning af dataansvarlig ved ulovlig instruks ▶ 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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens skabelon til indgåelse af databehandleraftaler med dataansvarlig og stikprøvevis indgåede databehandleraftaler med en dataansvarlig og observeret, at databehandleren er forpligtet til at underrette den dataansvarlige i tilfælde, hvor en instruks vurderes at være i strid med lovgivning.	Vi har konstateret, at der ikke har været tilfælde, hvor instruks har været vurderet i strid med lovgivning. Vi har derfor ikke kunnet teste kontrollens implementering og effektivitet. Ingen afvigelser konstateret.

Artikel 28, stk. 3, artikel 29, artikel 30, stk. 2, 3 og 4 og artikel 32, stk. 4: Databehandleraftale og behandling af personoplysninger på vegne af dataansvarliges instruks		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har på forespørgsel fået oplyst, at der ikke har været tilfælde i erklæringsperioden, hvor instruks har været vurderet i strid med lovgivning.	

Artikel 28, stk. 3, litra c: Opbevaring af personoplysninger		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Opbevaring af oplysninger er i overensstemmelse med dataansvarliges krav ▶ 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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Vi har stikprøvevis inspiceret på opbevaring af personoplysninger, at personoplysninger kun opbevares i den periode, som er aftalt med dataansvarlig. Vi har inspiceret, at procedurerne er opdateret og godkendt i erklæringsperioden.	Ingen afvigelser konstateret.
Lokation for behandling og opbevaring af oplysninger ▶ Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder for behandling og opbevaring af personoplysninger. Vi har stikprøvevis inspiceret på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser konstateret.

Artikel 28, stk. 2 og 4: Underdatabehandlere		
Kontrolmål ▶ *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.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Underdatabehandleraftale og instruks ▶ 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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Vi har inspiceret, at procedurerne er opdateret og godkendt i erklæringsperioden.	Ingen afvigelser konstateret.
Godkendelse af underdatabehandlere ▶ Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Vi har stikprøvevis inspiceret på underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlernes databehandling fremgår af indgåede databehandleraftaler med dataansvarlige.	Ingen afvigelser konstateret.
Ændringer i godkendte underdatabehandlere ▶ Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Vi har på forespørgsel fået oplyst, at der ikke er sket ændringer af underdatabehandlere i erklæringsperioden.	Vi har konstateret, at der ikke er sket ændringer af underdatabehandlere. Vi har derfor ikke kunnet teste kontrollens implementering og effektivitet. Ingen afvigelser konstateret.

Artikel 28, stk. 2 og 4: Underdatabehandlere		
Kontrolmål ▶ *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.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Underdatabehandlerens forpligtelser ▶ Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der er indgået databehandleraftaler med anvendte underdatabehandlere, Vi har stikprøvevis inspiceret underdatabehandleraftaler for, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen afvigelser konstateret.
Oversigt over underdatabehandlere ▶ Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: ○ Navn ○ CVR-nr. ○ Adresse ○ Beskrivelse af behandlingen	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Vi har inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen afvigelser konstateret.
Tilsyn med underdatabehandlere ▶ 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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Vi har inspiceret, at databehandleren har udført tilsyn, herunder indhentet og gennemgået underdatabehandlers revisorerklæringer. Vi har inspiceret, at databehandlerens tilsyn af underdatabehandlere ikke har givet anledning til yderligere handlinger.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra b: Fortrolighed og lovbestemt tavshedspligt		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Rekruttering af medarbejdere - Tavsheds- og fortrolighedsaftale med medarbejdere og introduktion til informationssikkerhed ▶ 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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har en proces for tavsheds- og fortrolighedsaftale.	Vi har konstateret, at der er etableret en procedure for rekruttering af medarbejdere. Vi har ikke kunnet udtale os om kontrollens implementering og effektivitet, da der ikke i erklæringsperioden har været tiltrædelser. Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Aftalte sikringsforanstaltninger ▶ 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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Vi har inspiceret, at procedurer er opdateret og godkendt i erklæringsperioden.	Ingen afvigelser konstateret.
Risikovurdering ▶ 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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har foretaget en risikovurdering baseret på potentielle risici for datas tilgængelighed, fortrolighed og integritet i forhold til den registreredes rettigheder. Vi har inspiceret, at den foretagne risikovurdering er opdateret og godkendt. Vi har stikprøvevis inspiceret, at databehandler har implementeret tekniske foranstaltninger på baggrund af risikovurderingen, herunder foranstaltninger der er aftalt med dataansvarlige.	Ingen afvigelser konstateret.
Antivirus ▶ Der er for de arbejdsstationer, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har stikprøvevis inspiceret, at for pc'er, der anvendes til behandling af personoplysninger, er der installeret antivirus, som er opdateret.	Ingen afvigelser konstateret.
Adgangsstyring - adgang til personoplysninger ▶ Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Vi har udført forespørgsel hos passende personale hos databehandleren.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Vi har inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger.	
Overvågning af systemer og miljøer ▶ Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter: ○ RAM og harddisk forbrug ○ MySQL forbindelser ○ Server oppetid (Pingdom)	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.	Ingen afvigelser konstateret.
Kryptering ved transmission af personoplysninger ▶ Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet.	Ingen afvigelser konstateret.
Logning ▶ Der er etableret logning i systemer, databaser og netværk af følgende forhold: ○ Aktiviteter, der udføres af brugere ○ Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder ○ Sikkerhedshændelser omfattende: ▪ Fejlede forsøg på log-on til systemer	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret. Vi har inspiceret, at logfiler har det forventede indhold i forhold til opsætning. Vi har inspiceret, at logfiler med systemadministratorer og andre med særlige rettigheders aktiviteter har det forventede indhold i forhold til opsætning.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Sårbarhedsscanninger og penetrationstests ▶ De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførsel af sårbarhedsscanninger og penetrationstests. Vi har inspiceret ved stikprøver, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger. Vi har inspiceret, at evt. afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret eller accepteret.	Ingen afvigelser konstateret.
Vedligeholdelse af systemsoftware ▶ Ændringer til arbejdsstationer og databaser følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret ved udtræk, at databaser er opdateret med relevante opdateringer og sikkerhedspatches. Vi har stikprøvevis inspiceret, at arbejdsstationer er opdateret med nyeste systemopdatering.	Ingen afvigelser konstateret.
Adgangsstyring - procedure og periodisk gennemgang ▶ Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Vi har inspiceret databehandlerens årshjul / procedure for brugerstyring, og observeret, at databehandleren regelmæssigt skal vurdere og godkende tildelte brugeradgange. Vi har inspiceret, at databehandleren har foretaget vurdering og godkendelse af brugeradgange.	Vi har konstateret, at der er etableret procedurer for tildeling og inddragelse af adgangsrettigheder. Vi har ikke kunnet udtale os om kontrollernes implementering og effektivitet, da der ikke i erklæringsperioden har været tiltrædelser eller fratrædelser. Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Logisk adgangskontrol ▶ Databehandleren har etableret regler for krav til adgangskoder, som skal følges af alle med adgang til personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at brugernes adgang til at udføre behandling af personoplysninger sker gennem adgangskoder, der afspejler risikoen ved behandlingsaktiviteten.	Ingen afvigelser konstateret.
Fysisk adgangskontrol ▶ Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til databehandlerens lokaler. Vi har inspiceret dokumentation for, at kun autoriserede personer har fysisk adgang til lokaler, hvori der behandles personoplysninger. Vi er på forespørgsel blevet oplyst, at databehandlerens personoplysninger bliver opbevaret hos hostingleverandørne. Vi har inspiceret hostingleverandørenes revisionserklæringer og observeret, at erklæringerne er uden forbehold og, at erklæringerne ikke indeholder forhold omkring fysisk adgangssikkerhed, som har krævet yderligere handlinger fra databehandleren.	Ingen afvigelser konstateret.
Sikkerhedskopiering og reetablering ▶ Databehandleren har etableret en procedure for sikkerhedskopiering og reetablering af data og systemer, der sikrer, at relevante systemer og data sikkerhedskopieres og opbevares på anden fysisk lokation, samt at systemer og data kan reetableres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer, der skal sikre sikkerhedskopiering og reetablering af relevante data og systemer, og at sikkerhedskopier opbevares på anden fysisk lokation. Vi har inspiceret, at der foretages sikkerhedskopiering af relevante systemer og data i overensstemmelse med proceduren.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har inspiceret, at sikkerhedskopier har været genetableret i erklæringsperioden.	
Fjernarbejdspladser og fjernadgang til systemer og data ▶ Fjernadgang til databehandlerens systemer og data sker via VPN-forbindelse.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens netværkstopologi og observeret, at der kun kan opnås fjernadgang til systemer og data via VPN. Vi har inspiceret dokumentation for, at adgang til VPN-forbindelsen sker via to-faktor autentifikation.	Ingen afvigelser konstateret.
Reparation-, service- og destruktion af it-udstyr ▶ Databehandleren har etableret en procedure for reparation-, service- og destruktion af it-udstyr, der sikrer sikker håndtering af it-udstyr indeholdende personoplysninger.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har formaliserede procedurer for reparation-, service- og destruktion af it-udstyr. VI har på forespørgsel fået oplyst, at der ikke har været sendt it-udstyr til reparation-, service- eller destruktion.	Vi har konstateret, at databehandleren ikke i erklæringsperioden har sendt it-udstyr til reparation-, service- eller destruktion. Vi har derfor ikke kunnet teste kontrollens implementering og effektivitet. Ingen afvigelser konstateret.

Artikel 25: Databeskyttelse gennem design og standardindstillinger		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer informationssikkerhed og databeskyttelse tilrettelægges og implementeres i databehandlerens udviklings- og ændringsproces.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Ændringsstyring og privacy-by-design ▶ Databehandleren har etableret en procedure for udviklings- og ændringsopgaver, der sikrer overholdelse af privacy-by-design-principperne, samt at alle udviklings- og ændringsopgaver følger en formaliseret proces, der sikrer test og krav om godkendelse inden implementering.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har etableret en procedure for udviklings- og ændringsopgaver, der sikrer overholdelse af privacy-by-design-principperne, samt at alle udviklings- og ændringsopgaver følger en formaliseret proces, der sikrer test og krav om godkendelse inden implementering. Vi har stikprøvevis for implementerede ændringer inspiceret, at udviklingsopgaverne har fulgt den formaliserede proces, og at der er udført test, og at udviklingerne er godkendt inden implementering.	Ingen afvigelser konstateret.
Implementering af ændring i produktionsmiljøet ▶ Databehandleren har etableret en procedure for implementering af ændringer i produktionsmiljøet, der sikrer funktionsadskillelse i implementeringsprocessen.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der er opsat funktionsadskillelse, således, at udviklere ikke kan implementere ændringer direkte i produktionsmiljøet uden at der foreligger en godkendelse	Ingen afvigelser konstateret.
Adskillelse af udviklings-, test- og produktionsmiljøet ▶ Udvikling og test udføres i udviklingsmiljøer, som er adskilte fra produktionsmiljøer.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at udviklings-, test- og produktionsmiljø er adskilte.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra g: Sletning og tilbagelevering af personoplysninger		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Sletning af oplysninger i overensstemmelse med dataansvarliges krav ▶ 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 en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Vi har inspiceret, at procedurerne er opdateret og godkendt i erklæringsperioden.	Ingen afvigelser konstateret.
Krav til opbevarings- og sletteperiode af oplysninger er i overensstemmelse med dataansvarliges krav ▶ Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutine.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at de foreliggende procedurer for opbevaring og sletning af personoplysninger indeholder specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Vi har inspiceret ved stikprøver på databehandlinger fra databehandlerens fortegnelse over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder.	Ingen afvigelser konstateret.
Sletning og tilbagelevering ved ophør af kundeforhold ▶ 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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer for tilbagelevering og/eller sletning af den dataansvarliges data ved ophør af behandling af personoplysninger. Vi har på forespørgsel fået oplyst, at der individuelt aftales med kunden, hvordan behandlingen afvikles.	Vi har konstateret, at der ikke i erklæringsperioden har været ophør af databehandleraftaler. Vi har derfor ikke kunnet teste kontrollens implementering og effektivitet. Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra g: Sletning og tilbagelevering af personoplysninger		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har på forespørgsel fået oplyst, at der ikke har været ophør af databehandleraftaler.	

Artikel 28, stk. 3, litra e, f og h: Bistand til den dataansvarlige		
Kontrolmål ▶ *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.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Procedure for opfyldelse af registreredes rettigheder ▶ 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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Vi har inspiceret, at procedurerne er opdateret og godkendt.	Ingen afvigelser konstateret.
Tekniske foranstaltninger til opfyldelse af registreredes rettigheder ▶ 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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har 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. Vi har inspiceret dokumentation for, at de anvendte systemer understøtter gennemførelsen af de nævnte detaljerede procedurer. Vi har på forespørgsel fået oplyst, at der ikke er sket anmodning om bistand i forhold til de registreredes rettigheder.	Vi har konstateret, at der ikke i erklæringsperioden er sket anmodning om bistand i forhold til de registreredes rettigheder. Vi har derfor ikke kunnet teste kontrollens implementering og effektivitet. Ingen afvigelser konstateret.

Artikel 30, stk. 2, 3 og 4: Fortegnelse over kategorier af behandlingsaktiviteter		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Fortegnelse over behandlingsaktiviteter ▶ Databehandleren har etableret en fortegnelse over kategorier af behandlingsaktiviteter som databehandler. Fortegnelsen skal indeholde: o navn og kontaktoplysninger for dataansvarlige, o de kategorier af behandling, der foretages på vegne af dataansvarlige, o navn og kontaktoplysninger for hver underdatabehandler, o angivelse af eventuel overførsel af personoplysninger til et tredjeland. ▶ Fortegnelsen opbevares elektronisk og stilles til rådighed for tilsynsmyndigheden efter anmodning.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret databehandlerens fortegnelse over kategorier af behandlingsaktiviteter som databehandler og observeret, at den indeholder relevante oplysninger, samt at fortegnelsen bliver opbevaret elektronisk. Vi har inspiceret, at fortegnelsen er opdateret og/eller godkendt. Vi har på forespørgsel fået oplyst, at Datatilsynet ikke har anmodet om udlevering af fortegnelsen i erklæringsperioden.	Vi har konstateret, at Datatilsynet ikke ved erklæringstidspunktet har anmodet om udlevering af fortegnelsen. Vi har derfor ikke kunnet teste kontrollens implementering og effektivitet. Ingen afvigelser konstateret.

Artikel 33, stk. 2: Underretning om brud på persondatasikkerheden		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Underretning om brud på persondatasikkerhed ▶ 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.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Vi har inspiceret, at proceduren er opdateret og godkendt i erklæringsperioden.	Ingen afvigelser konstateret.
Identifikation af brud på persondatasikkerhed ▶ Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: ○ Awareness hos medarbejdere ○	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandler udbyder awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.	Ingen afvigelser konstateret.
Rettidig underretning om brud på persondatasikkerhed ▶ Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 24 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Vi har observeret, at der ikke har været konstateret hændelser, som har medført brud på persondatasikkerheden i erklæringsperioden.	Vi har konstateret, at der ikke i erklæringsperioden har været konstateret hændelser, som har medført brud på persondatasikkerheden. Vi har derfor ikke kunnet teste kontrollens implementering og effektivitet. Ingen afvigelser konstateret.

Artikel 33, stk. 2: Underretning om brud på persondatasikkerheden		
Kontrolmål ▶ *Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Bistand til dataansvarlige ved brud på persondatasikkerhed ▶ Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: ▶ Karakteren af bruddet på persondatasikkerheden ▶ Sandsynlige konsekvenser af bruddet på persondatasikkerheden ▶ Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for: • 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. Vi har inspiceret dokumentation for, at der ved brud på persondatasikkerheden er truffet foranstaltninger, som har håndteret bruddet på persondatasikkerheden. Vi har observeret, at der ikke har været konstateret hændelser, som har medført brud på persondatasikkerheden i erklæringsperioden.	Vi har konstateret, at der ikke i erklæringsperioden har været konstateret hændelser, som har medført brud på persondatasikkerheden. Vi har derfor ikke kunnet teste kontrollens implementering og effektivitet. Ingen afvigelser konstateret

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk

PENNEO

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

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

Martin Saldern Schrøder
Direktør/Partner
På vegne af: Compaya
Serienummer: e227fbdb-8ee7-42c5-94e0-69223948aaf3
IP: 2.66.xxx.xxx
2025-07-04 08:55:28 UTC

Mikkel Jon Larssen
BDO Holding VII, statsautoriseret revisionsaktieselskab CVR: 20222670
Partner, chef for Risk Assurance, CISA, CRISC
På vegne af: BDO
Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff
IP: 77.243.xxx.xxx
2025-07-04 08:56:46 UTC

Nicolai Tobias Visti Pedersen
BDO Holding VII, statsautoriseret revisionsaktieselskab CVR: 20222670
Statsautoriseret revisor
På vegne af: BDO
Serienummer: 375cad19-f0ea-4e39-8646-d3d882b8ce8e
IP: 37.96.xxx.xxx
2025-07-04 08:58:01 UTC