Compaya A/S

Palægade 4, 2. tv.
1261 København K
CVR.NR. 31 37 54 28

ISAE 3000, type 2

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om beskrivelsen af kontroller rettet mod databeskyttelse og behandling af personoplysninger for perioden 1. juni 2025 – 31. maj 2026.

Indhold

S.nr. 302391

AOG/JR

1. Ledelsens udtalelse

Compaya A/S varetager behandling af personoplysninger på vegne af vores kunder, der er dataansvarlige i henhold til indgåede databehandleraftaler.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt Compaya A/S' SMS-systemer, 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 kaldet "databeskyttelsesforordningen") er overholdt.

Compaya A/S anvender team.blue Denmark A/S og Rackhosting ApS som underdatabehandlere for anvendt hosting og netværk. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som team.blue Denmark A/S og Rackhosting ApS varetager for Compaya A/S.

Enkelte af de kontrolmål, der er ført i beskrivelsen i afsnit 2, kan kun nås, hvis de komplementærekontroller hos Compaya A/S' kunder er hensigtsmæssigt udformet og fungerer effektivt sammen med vores kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementære kontroller.

Compaya A/S bekræfter, at:

a) Den medfølgende beskrivelse, i afsnit 2, giver en retvisende beskrivelse af Compaya A/S' ydelse, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen i hele perioden 1. juni 2025 til 31. maj 2026. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan Compaya A/S' systemer 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 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

(ii) Indeholder relevante oplysninger om ændringer ved ydelsen til behandling af personoplysninger foretaget i perioden 1. juni 2025 til 31. maj 2026.

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne ydelse 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 ydelsen, 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 hensigtsmæssigt udformet og fungerede effektivt i hele perioden 1. juni 2025 til 31. maj 2026. 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 i hele perioden fra 1. juni 2025 til 31. maj 2026.

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.

København K, den 25. august 2026
Compaya A/S

Martin Saldern Schrøder
Direktør

2. 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. 8 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 bruger-roller, 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 kontrolaktiviteter:

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
<u>Risikovurdering</u>
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.

<u>Beredskabsplaner</u>
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 brugeridentifikation 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.

Ændringer i erklæringsperioden

Compaya har i erklæringsperioden skiftet revisor, og dermed kan strukturen i erklæringen være lidt anderledes end i tidligere erklæringer.

3. Uafhængig revisors ISAE 3000-erklæring med sikkerhed om beskrivelsen af kontroller rettet mod databeskyttelse og behandling af personoplysninger

Til ledelsen hos Compaya A/S og deres kunder

Omfang
Vi har fået som opgave at afgive erklæring om Compaya A/S' beskrivelse i afsnit 2 af ydelse til behandling af personoplysninger i henhold til databehandleraftaler med dataansvarlige, i hele perioden 1. juni 2025 til 31. maj 2026 (beskrivelsen) og om udformningen og funktionen af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Compaya A/S anvender team.blue Denmark A/S og Rackhosting ApS som underdatabehandlere for anvendt hosting og netværk. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som team.blue Denmark A/S og Rackhosting ApS varetager for Compaya A/S.

Enkelte af de kontrolmål, der er ført i beskrivelsen i afsnit 2, kan kun nås, hvis de komplementærekontroller hos Compaya A/S' kunder er hensigtsmæssigt udformet og fungerer effektivt sammen med vores kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementære kontroller.

Compaya A/S' ansvar
Compaya A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for at udforme, 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, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

Vores revisionsfirma anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementere 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 Compaya A/S' beskrivelse samt om udformningen 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. 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 funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af sin ydelse 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 omfattet test af funktionaliteten 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 mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i afsnit 1.

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
Compaya 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 i afsnit 1. Det er vores opfattelse,

(a) at beskrivelsen af ydelsen, således som denne var udformet og implementeret i hele perioden fra 1. juni 2025 til 31. maj 2026, i alle væsentlige henseender er retvisende, og
(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. juni 2025 til 31. maj 2026,
(c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. juni 2025 til 31. maj 2026.

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

Tiltænkte brugere og formål
Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt dataansvarlige, der har anvendt Compaya 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.

Søborg, den 25. august 2026

inforevision
statsautoriseret revisionsaktieselskab

John Richardt Søbjærg
statsautoriseret revisor

Simon Okkels
Partner, Lead IT-auditor (CISA)

4. Kontrolmål, kontrolaktiviteter, test og resultat heraf

4.1 Formål og omfang

Vores arbejde er udført i overensstemmelse med ISAE 3000, *Andre erklæringer med sikkerhed end revision eller review af historiske finansielle oplysninger.*

Den følgende oversigt er udformet for at skabe en forståelse for effektiviteten af de kontroller, som Compaya A/S har implementeret. Vores test af funktionaliteten har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, som vi har vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål har været opnået i hele perioden 1. juni 2025 til 31. maj 2026.

Denne erklæring er afgivet efter den partielle metode, og omfatter ikke kontrolmål og tilknyttede kontroller hos Compaya A/S' underleverandører og underdatabehandlere.

Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos Compaya A/S' kunder er ikke omfattet af vores testhandlinger.

4.2 Udførte testhandlinger

De udførte testhandlinger i forbindelse med fastlæggelsen af kontrolaktiviteternes funktionalitet er beskrevet nedenfor:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel til passende personale hos Compaya A/S er udført for alle væsentlige kontrolaktiviteter. Forespørgsler er udført for blandt andet at opnå viden og yderligere oplysninger om indførte politikker og procedurer, herunder hvordan kontrolaktiviteterne udføres. Endvidere for at få bekræftet beviser for politikker, procedurer og kontroller.
Inspektion	Gennemgang og stillingtagen til politikker, procedurer og dokumentation, som indeholder information om udførelse af kontrollen. Det omfatter gennemlæsning og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Observation	Observation af kontrollens udførelse.
Genudførelse af kontrol	Den relevante kontrol er genudført med henblik på at verificere, at kontrollen fungerer som forventet

Beskrivelse og resultat af vores test af de testede kontroller fremgår af de efterfølgende skemaer. I det omfang vi har konstateret væsentlige svagheder i kontrolmiljøet eller afvigelser herfra, har vi anført dette.

Kontrolmål A (Instruks) Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.			
Nr.	Compaya A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
A1	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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Inspiceret, at procedurer er opdateret.	Vi har ikke konstateret afvigelser.
A2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret via stikprøver på behandling af personoplysninger, at disse foregår i overensstemmelse med instruks.	Vi har ikke konstateret afvigelser.
A3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Inspiceret, at den dataansvarlige er underrettet i tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.	Vi er blevet oplyst om at der ikke har været tilfælde hvor virksomheden har vurderet instruksen værende i strid med lovgivningen Vi har ikke konstateret afvigelser.

Kontrolmål B (Tekniske foranstaltninger) Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	Compaya A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B1	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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Inspiceret, at procedurer er opdateret. Inspiceret via stikprøver på indgåede databehandleraftaler, at der er etableret de aftalte sikringsforanstaltninger.	Vi har ikke konstateret afvigelser.
B2	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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed. Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Inspiceret, at databehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Inspiceret, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.	Vi har ikke konstateret afvigelser.
B3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus software. Inspiceret, at antivirus software er opdateret.	Vi har ikke konstateret afvigelser.
B4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Inspiceret, at firewall er konfigureret i henhold til intern politik herfor.	Vi har ikke konstateret afvigelser.

Kontrolmål B (Tekniske foranstaltninger) Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	Compaya A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Inspiceret netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering.	Vi har ikke konstateret afvigelser.
B6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger. Inspiceret via stikprøver på brugeres adgange til systemer og databaser, at de er begrænset til medarbejdernes arbejdsbetingede behov.	Vi har ikke konstateret afvigelser.
B7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering. Inspiceret, at der via stikprøver på alarmer er sket opfølgning, samt at forholdet er meddelt de dataansvarlige i behørigt omfang.	Vi har ikke konstateret afvigelser.

Kontrolmål B (Tekniske foranstaltninger) Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	Compaya A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme. Inspiceret, at teknologiske løsninger til kryptering har været tilgængelige og aktiveret i hele erklæringsperioden. Inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail.	Vi har ikke konstateret afvigelser.
B9	Der er etableret logning i systemer, databaser og netværk. F.eks.: aktiviteter udført af administratorer, sikkerhedshændelser som ændringer i log indstillinger, deaktivering af logning, ændringer i brugerrettigheder, fejlede loginforsøg. Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang og opfølgning på logs. Inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret. Inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning. Inspiceret via stikprøver på logning, at logfiler har det forventede indhold i forhold til opsætning, og at der er dokumentation for den foretagne opfølgning og håndtering af evt. sikkerhedshændelser. Inspiceret via stikprøver på logning, at der er dokumentation for den foretagne opfølgning på aktiviteter udført af systemadministratorer og andre med særlige rettigheder.	Vi har ikke konstateret afvigelser.

Kontrolmål B (Tekniske foranstaltninger) Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	Compaya A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form. Inspiceret via stikprøve på udviklings- og testdatabaser, at personoplysninger heri er pseudonymiseret eller anonymiseret.	Vi har ikke konstateret afvigelser.
B11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførsel af sårbarhedsscanninger og penetrationstests. Inspiceret ved stikprøver, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger. Inspiceret, at evt. afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret samt meddelt de dataansvarlige i behørigt omfang.	Vi har ikke konstateret afvigelser.
B12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Inspiceret ved udtræk af tekniske sikkerhedsparametre og -opsætninger, at systemer, databaser og netværk er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.	Vi har ikke konstateret afvigelser.

Kontrolmål B (Tekniske foranstaltninger)

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

Nr.	Compaya A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B13	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.	Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Inspiceret via stikprøve på medarbejderes adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov. Inspiceret via stikprøve på fratrådte medarbejdere, at disses adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Inspiceret, at der foreligger dokumentation for regelmæssig - mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.	Vi har konstateret, at processen for deaktivering af adgange for én fratrådt medarbejder samt det efterfølgende brugerreview ikke har fungeret effektivt i perioden, idet adgangen til ét system, der anvendes til intern kommunikation, ikke blev deaktiveret rettidigt. Ingen yderligere afvigelser fundet.
B14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor autentifikation.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at to-faktor autentifikation anvendes ved behandling af personoplysninger, der medfører højrisiko for de registrerede. Inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører høj-risiko for de registrerede, alene kan ske ved anvendelse af to-faktor autentifikation.	Vi har ikke konstateret afvigelser.
B15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Inspiceret dokumentation for, at kun autoriserede personer har haft fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger, i erklæringsperioden.	Vi har ikke konstateret afvigelser.

Kontrolmål C (Organisatoriske foranstaltninger) Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	Compaya A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
C1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Vi har ikke konstateret afvigelser.
C2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Inspiceret via stikprøve på indgåede databehandleraftaler, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Vi har ikke konstateret afvigelser.
C3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: Referencer fra tidligere ansættelser, straffeattest, eksamensbeviser m.v.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Inspiceret via stikprøve på databehandleraftaler, at kravene til efterprøvning af medarbejdere i aftalerne er dækket af databehandlerens procedurer for efterprøvning. Inspiceret via stikprøve på nyansatte medarbejdere i erklæringsperioden, at der er dokumentation for, at efterprøvningen har omfattet referencer fra tidligere ansættelser, straffeattest, eksamensbeviser m.v., i relevant omfang.	Vi er blevet oplyst om, at der ikke har været nyansættelser i perioden. Det har derfor ikke været muligt at teste kontrollens effektivitet. Vi har ikke konstateret afvigelser.

Kontrolmål C (Organisatoriske foranstaltninger) Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	Compaya A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
C4	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 ved en stikprøve på nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere har underskrevet en fortrolighedsaftale. Inspiceret ved en stikprøve på nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere er blevet introduceret til: informationssikkerhedspolitikken, procedurer vedrørende databehandlings, samt anden relevant information.	Vi er blevet oplyst om, at der ikke har været nyansættelser i perioden. Det har derfor ikke været muligt at teste kontrollens effektivitet. Vi har ikke konstateret afvigelser.
C5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages Inspiceret ved en stikprøve på fratrådte medarbejdere i erklæringsperioden, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.	Vi har konstateret, at processen for deaktivering af adgange for en enkelt fratrådt medarbejder, ikke har fungeret effektivt i perioden. Ingen yderligere afvigelser fundet.
C6	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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Inspiceret ved en stikprøve på fratrådte medarbejdere i erklæringsperioden, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt.	Vi har ikke konstateret afvigelser.
C7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.	Vi har ikke konstateret afvigelser.

Kontrolmål D (Sletning og tilbagelevering) Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.			
Nr.	Compaya A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
D1	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.	Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Inspiceret, at procedurerne er opdateret.	Vi har ikke konstateret afvigelser.
D2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder. Inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger er slettet i overensstemmelse med de aftalte sletterutiner.	Vi har ikke konstateret afvigelser.
D3	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.	Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Inspiceret ved en stikprøve på ophørte databehandlinger i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	Vi har ikke konstateret afvigelser.

Kontrolmål E (Opbevaring) Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.			
Nr.	Compaya A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
E1	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.	Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Inspiceret, at procedurerne er opdateret. Inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Vi har ikke konstateret afvigelser.
E2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Inspiceret ved en stikprøve på 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.	Vi har ikke konstateret afvigelser.

Kontrolmål F (Underdatabehandlere) Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.			
Nr.	Compaya A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
F1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Vi har ikke konstateret afvigelser.
F2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Inspiceret ved en stikprøve på underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Vi har ikke konstateret afvigelser.
F3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	Vi har fået oplyst, at der ikke er skiftet underdatabehandlere i perioden, og har derfor ikke kunne teste effektiviteten af kontrollen. Vi har ikke konstateret afvigelser.
F4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Inspiceret ved en stikprøve på underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Vi har ikke konstateret afvigelser.

Kontrolmål F (Underdatabehandlere)

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

Nr.	Compaya A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
F5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: Navn, CVR-Nr., Adresse, beskrivelse af behandlingen.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Vi har ikke konstateret afvigelser.
F6	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.	Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende.	Vi har ikke konstateret afvigelser.

Kontrolmål G (Tredjelandsoverførsler) 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.	Compaya A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
G1	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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at personoplysninger alene overføres til tredjelande eller internationale organisationer i henhold til aftale med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Inspiceret, at procedurerne er opdateret.	Vi er blevet oplyst om at der ikke for nogle kundeløsninger er aftaler om at virksomheden må overføre data til tredjelande Vi har ikke konstateret afvigelser.
G2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer. Inspiceret ved en stikprøve på dataoverførsler fra databehandlerens oversigt over overførsler, at der er dokumentation for, at overførslen er aftalt med den dataansvarlige i databehandleraftalen eller senere godkendt.	Vi er blevet oplyst om at der ikke for nogle kundeløsninger er aftaler om at virksomheden må overføre data til tredjelande Vi har ikke konstateret afvigelser.
G3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Inspiceret, at der foreligger formaliserede procedurer for sikring af et gyldigt overførselsgrundlag. Inspiceret, at procedurerne er opdateret. Inspiceret ved en stikprøve på dataoverførsler 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.	Vi er blevet oplyst om at der ikke for nogle kundeløsninger er aftaler om at virksomheden må overføre data til tredjelande Vi har ikke konstateret afvigelser.

Kontrolmål H (Registreredes rettigheder) 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.	Compaya A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
H1	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.	Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.	Vi har ikke konstateret afvigelser.
H2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer. Inspiceret, at dokumentation for anmodninger om bistand fra den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede er korrekt og rettidigt gennemført.	Vi har fået oplyst, at der ikke har været udført bistand til dataansvarlig i perioden, og har derfor ikke kunne teste effektiviteten af kontrollen. Vi har ikke konstateret afvigelser.

Kontrolmål I (Sikkerhedsbrud) Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.			
Nr.	Compaya A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
I1	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.	Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at proceduren er opdateret.	Vi har ikke konstateret afvigelser.
I2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejdere, • overvågning af netværkstrafik, • opfølgning på logning af tilgang til personoplysninger.	Inspiceret, at databehandler udbyder awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Inspiceret dokumentation for, at netværkstrafik overvåges, samt at der sker opfølgning på anormaliteter, overvågningsalarmer, overførsel af store filer mv. Inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang.	Vi har ikke konstateret afvigelser.
I3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 72 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Forespurgt underdatabehandlerne, om de har konstateret nogen brud på persondatasikkerheden i erklæringsperioden Inspiceret, at databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser. Inspiceret, at samtlige registrerede brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødig forsinkelse og senest 72 timer efter, at databehandleren er blevet opmærksom på brud på persondatasikkerheden.	Vi er blevet oplyst om, at der ikke har været nogen brud på persondatasikkerheden i erklæringsperioden. Vi har ikke konstateret afvigelser.

Kontrolmål I (Sikkerhedsbrud) Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.			
Nr.	Compaya A/S' kontrolaktivitet	Revisors udførte test	Resultat af revisors test
I4	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.	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. Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden. Inspiceret dokumentation for, at der ved brud på persondatasikkerheden er truffet foranstaltninger, som har håndteret bruddet på persondatasikkerheden.	Vi har ikke konstateret afvigelser.

5. Ledelsens kommentarer til "resultat af revisors test"

Compaya A/S har følgende redegørelse for resultatet af erklæringen:

Nr.	*Compaya A/S' kontrolaktivitet*	*Resultat af revisors test*	*Ledelsens svar*
B13	Der er formaliseret forretningsgang for tildeling og afbrydelse af bruger adgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Vi har konstateret, at processen for deaktivering af adgange for én fratrådt medarbejder samt det efterfølgende brugerreview ikke har fungeret effektivt i perioden, idet adgangen til ét system, der anvendes til intern kommunikation, ikke blev deaktiveret rettidigt.	Det drejer sig om systemet Slack, der alene benyttes til intern kommunikation.
C5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Vi har konstateret, at processen for deaktivering af adgange for en enkelt fratrådt medarbejder, ikke har fungeret effektivt i perioden.	Det drejer sig om systemet Slack, der alene benyttes til intern kommunikation.

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
Serienummer: e227fbdb-8ee7-42c5-94e0-69223948aaf3
IP: 152.115.xxx.xxx
2026-08-25 08:32:17 UTC

Mit ID

Simon Okkels
inforevision statsautoriseret revisionsaktieselskab CVR: 19263096
Partner, Lead IT-auditor (CISA)
Serienummer: 7ced0dfc-fff1-4f9c-a5b4-e6fcd672bf9a
IP: 93.165.xxx.xxx
2026-08-25 08:41:29 UTC

Mit ID

John Richardt Søbjærg
inforevision statsautoriseret revisionsaktieselskab CVR: 19263096
Statsautoriseret revisor
På vegne af: inforevision a/s
Serienummer: 70a986b1-9464-4830-8fb8-b43b6517911a
IP: 93.165.xxx.xxx
2026-08-25 08:55:35 UTC

Mit ID