



COMPAYA A/S

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

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING	2
2. COMPAYA A/S' UDTALELSE	4
3. COMPAYA A/S' BESKRIVELSE AF COMPAYAS SMS-SYSTEMER	6
4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST	12
Artikel 28, stk. 1: Databehandlerens garantier	15
Artikel 28, stk. 3: Databehandleraftale	18
Artikel 28, stk. 3 og 10, artikel 29 og artikel 32, stk. 4: Instruks for behandling af personoplysninger.....	19
Artikel 28, stk. 2 og 4: Underdatabehandlere	20
Artikel 28, stk. 3, litra b: Fortrolighed og lovbestemt tavshedspligt	22
Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger	23
Artikel 25: Databeskyttelse gennem design og standardindstillinger	29
Artikel 28, stk. 3, litra g: Sletning og tilbagelevering af personoplysninger	30
Artikel 28, stk. 3, litra e, f og h: Bistand til den dataansvarlige	31
Artikel 30, stk. 2, 3 og 4: Fortegnelse over kategorier af behandlingsaktiviteter	34
Artikel 33, stk. 2: Underretning om brud på persondatasikkerheden	35

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 15. MAJ 2024 OM BESKRIVELSEN AF COMPAYAS SMS-SYSTEMER OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING, 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) pr. 15. maj 2024 udarbejdede beskrivelse i sektion 3 af Compayas 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 af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vi har ikke udført handlinger vedrørende den operationelle effektivitet af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

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 og implementere 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 revisors 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 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.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens

beskrivelse samt for kontrollernes udformning. 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. 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.

Som nævnt ovenfor har vi ikke udført handlinger vedrørende den operationelle effektivitet af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

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

Begrænsninger i kontroller hos en databehandler

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 Compayas 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.

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 Compayas 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 pr. 15. maj 2024, 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 pr. 15. maj 2024.

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 Compayas 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 4. juni 2024

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 Compayas 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 Compayas 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 underdatabehandlers 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 Compayas SMS-systemer og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller pr. 15. maj 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for Compayas 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 Compayas 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 Compayas 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 Compayas SMS-systemer, som den enkelte dataansvarlige måtte anse vigtigt 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 pr. 15. maj 2024. 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.

Compaya A/S bekræfter, at der er implementeret 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 4. juni 2024

Compaya A/S

Martin Saldern Schrøder
Direktør/Partner

3. COMPAYA A/S' BESKRIVELSE AF COMPAYAS 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 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 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 databehandlerkik 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.

Databehandlersaftaler

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 databehandlersaftaler i overensstemmelse med de tjenester, der leveres, herunder information om brugen af underdatabehandlere. Databehandlersaftalerne underskrives af begge parter og opbevares elektronisk.

Compaya udfører som databehandler kun behandling af personoplysninger efter dokumenteret instruks fra den dataansvarlige, enten i databehandlersaftalen 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 revisionsfirma angående underdatabehandlerens 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 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.

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 den IT-sikkerhedsansvarlige, 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 unødigt 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 lovlige 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.
- Ansvar 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 Compayas 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.

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 pr. 15. maj 2024.

Udførte testhandlinger

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

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 implementerede, 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.

For de ydelser, som Rackhosting ApS leverer inden for hostingydelser, har vi modtaget en ISAE 3000-erklæring om informationssikkerhed og foranstaltninger for perioden 1. maj 2022 til 30. april 2023 i henhold til data-behandleraftale.

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 2023.

Disse underdatabehandlers relevante kontrolmål og tilknyttede kontroller indgår ikke i Compaya A/S' beskrivelse af Compayas 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 eller implementeret.

Artikel 28, stk. 1: Databehandlerens garantier		
Kontrolmål ▶ At sikre, at databehandleren kan stille de fornødne garantier til beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og beskyttelsen af den registreredes rettigheder.		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Informationssikkerhedspolitik <ul style="list-style-type: none"> ▶ Compaya's har udarbejdet og implementeret en informationssikkerhedspolitik. ▶ Compaya's har udarbejdet og implementeret en databeskyttelsespolitik. 	Vi har udført forespørgsel hos passende personale hos databehandleren. Vi har foretaget inspektion af Compaya's informationssikkerhedspolitik. Vi har foretaget inspektion af Compaya's persondatapolitik for Compayas SMS-systemer (CPSMS.dk, ProSMS.se/SMS.dk).	Ingen afvigelser konstateret.
Gennemgang af informationssikkerhedspolitik <ul style="list-style-type: none"> ▶ Compaya's informationssikkerhedspolitik og persondatapolitik bliver gennemgået og opdateret minimum en gang årligt. ▶ Der er etableret et IT-sikkerhedsudvalg, som foretager gennemgang og godkendelse af informationssikkerhedspolitikken og it-sikkerhedshåndbogen. 	Vi har udført forespørgsel hos passende personale hos Compaya. Vi har inspiceret, at der er udarbejdet et årshjul, som medvirker til at sikre, at informationssikkerhedspolitik og persondatapolitik bliver gennemgået og opdateret minimum en gang årligt. Vi har inspiceret, at Compaya's informationssikkerhedspolitik senest er godkendt af ledelsen i august 2023, og at der er foretaget vurdering af behov for opdatering af persondatapolitik, hvorefter persondatapolitik for ProSMS.se/SMS.dk og CPSMS.dk senest er opdateret i august 2023. Vi har inspiceret, at der er etableret et IT-sikkerhedsudvalg. Vi har foretaget inspektion af dokumentation, som bekræfter, at IT-sikkerhedsudvalget foretager gennemgang og godkendelse af informationssikkerhedspolitikken og den tilhørende it-sikkerhedshåndbog.	Ingen afvigelser konstateret.

Artikel 28, stk. 1: Databehandlerens garantier		
Kontrolmål ▶ At sikre, at databehandleren kan stille de fornødne garantier til beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og beskyttelsen af den registreredes rettigheder.		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Rekruttering af medarbejdere ▶ Compaya har udarbejdet og implementeret en procedure for rekruttering af nye medarbejdere, herunder screening af medarbejder før ansættelse.	Vi har udført forespørgsel hos passende personale hos Compaya. Vi har foretaget inspektion af procedure for rekruttering af nye medarbejdere. Vi har inspiceret at databehandleren har udført screening af den seneste ansatte medarbejder før ansættelsen.	Ingen afvigelser konstateret.
Fratrædelse af medarbejdere ▶ Compaya har udarbejdet og implementeret en procedure for fratrædelse af medarbejdere ved ophør af ansættelsen. Ledelsen skal sikre, at proceduren bliver overholdt og dokumenteret.	Vi har udført forespørgsel hos passende personale hos Compaya. Vi har foretaget inspektion af procedure for fratrædelse af medarbejdere ved ophør af ansættelsen. Vi har inspiceret at databehandleren har fulgt proceduren for fratrædelse af medarbejder ved ophør af ansættelsen for den seneste fratrådte medarbejder.	Ingen afvigelser konstateret.
Uddannelse, awareness og oplysningskampagner for medarbejdere ▶ Compaya sikrer, at medarbejderne bliver informeret om procedurer og politikker angående behandling af personoplysninger. ▶ Compaya udfører løbende awareness-kampagner i form af opslag, møder og e-mails mv.	Vi har udført forespørgsel hos passende personale hos Compaya. Vi har foretaget inspektion af it-sikkerhedshåndbogen. Vi har foretaget inspektion af procedure for uddannelse af medarbejdere, hvor der fremgår bestemmelser om, at medarbejdere skal have kendskab til informationssikkerhedspolitikken og it-sikkerhedshåndbogen, herunder bestemmelserne angående behandling af personoplysninger.	Ingen afvigelser konstateret.

Artikel 28, stk. 1: Databehandlerens garantier**Kontrolmål**

- *At sikre, at databehandleren kan stille de fornødne garantier til beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og beskyttelsen af den registreredes rettigheder.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har foretaget inspektion af dokumentation, som bekræfter, at der udføres løbende awareness-kampagner i form af online kurser og e-mails mv.	

Artikel 28, stk. 3: Databehandleraftale		
Kontrolmål ► <i>At sikre, at databehandleren indgår en skriftlig kontrakt med den dataansvarlige, der fastsætter vilkårene for behandlingen af den dataansvarliges personoplysninger, og at kontrakten opbevares elektronisk.</i>		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Indgåelse af databehandleraftale med den dataansvarlige <ul style="list-style-type: none"> ► Compaya har procedure for indgåelse af skriftlige databehandleraftaler, der er i overensstemmelse med de ydelser, som databehandleren leverer. ► Compaya anvender en aftaleskabelon ved indgåelse af databehandleraftaler. ► Databehandleraftaler underskrives og opbevares elektronisk. ► Databehandleraftaler indeholder informationer om brugen af underdatabehandlere. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af procedure for indgåelse af skriftlige databehandleraftaler, der er i overensstemmelse med de ydelser, som Compaya leverer.</p> <p>Vi har inspiceret, at Compaya har udarbejdet en aftaleskabelon ved indgåelse af databehandleraftaler. Det er vores vurdering, at aftaleskabelonen opfylder kravene i databeskyttelsesforordningens artikel 28. stk. 3.</p> <p>Vi har foretaget inspektion af dokumentation, som bekræfter, at databehandleraftaler underskrives og opbevares elektronisk.</p> <p>Vi har foretaget inspektion af en indgået databehandleraftale for henholdsvis CPSMS.dk og ProSMS.se/SMS.dk og set at databehandleraftalerne indeholder informationer om brugen af underdatabehandlere.</p>	<p>Ingen afvigelser konstateret.</p>

Artikel 28, stk. 3 og 10, artikel 29 og artikel 32, stk. 4: Instruks for behandling af personoplysninger		
Kontrolmål ▶ At sikre, at databehandleren alene handler efter dokumenteret instruks fra den dataansvarlige. ▶ At sikre, at databehandleren underretter den dataansvarlige, hvis en instruks er i strid med databeskyttelsesforordningen og databeskyttelsesloven.		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Instruks for behandling af personoplysninger ▶ Compaya sikrer, at indgåede databehandleraftaler indeholder en instruks fra de dataansvarlige. ▶ Compaya udfører alene behandling af personoplysninger, som fremgår af instruks fra dataansvarlig. ▶ Compaya har udarbejdet og implementeret skriftlige procedurer vedrørende behandling af personoplysninger, så der alene behandles efter instruks fra dataansvarlig.	Vi har udført forespørgsel hos passende personale hos Compaya. Vi har inspiceret, at der er udarbejdet en aftaleskabelon ved indgåelse af databehandleraftaler. Vi har foretaget inspektion af Compayas procedurer vedrørende behandling af personoplysninger hvor det fremgår, at personoplysningerne skal behandles i overensstemmelse med instruks fra dataansvarlig. Vi har foretaget inspektion af én stikprøve for en databehandleraftaler for henholdsvis CPSMS.dk, ProSMS.se og SMS.dk og set, at databehandleraftalerne indeholder en instruks fra de dataansvarlige.	Ingen afvigelser konstateret.
Underretning af den dataansvarlige ved ulovlig instruks ▶ Databehandleraftale indeholder vilkår om, at den dataansvarlige skal informeres om instruktioner, der strider mod lovgivningen.	Vi har udført forespørgsel hos passende personale hos Compaya. Vi har inspiceret, at der er udarbejdet en aftaleskabelon ved indgåelse af databehandleraftaler. Vi har foretaget inspektion af én stikprøve for en indgået databehandleraftale for henholdsvis CPSMS.dk, ProSMS.se og SMS.dk og set, at databehandleraftalerne indeholder vilkår om, at den dataansvarlige skal informeres om instruktioner, der strider mod lovgivningen. Vi har på forespørgsel fået oplyst, at der ikke har været eksempler på databehandleraftaler, som er i strid med lovgivningen, hvorfor det ikke har været muligt at teste implementeringen af den indførte kontrol.	Ingen afvigelser konstateret.

Artikel 28, stk. 2 og 4: Underdatabehandlere		
<p>Kontrolmål</p> <ul style="list-style-type: none"> ▶ At sikre, at underdatabehandleren er pålagt de samme databeskyttelsesforpligtelser, som databehandleren er pålagt af den dataansvarlige, ved indgåelse af en skriftlig kontrakt med tilhørende instruks. ▶ At sikre, at den dataansvarlige har givet en forudgående specifik eller generel skriftlig godkendelse af underdatabehandlere. ▶ At sikre, at underdatabehandleren kan stille de fornødne garantier til beskyttelse af personoplysningerne i overensstemmelse med kontrakten. 		
Kontrolaktivitet	Test udført af BDO	Resultat af test
<p>Aftale med underdatabehandlere og leverandører</p> <ul style="list-style-type: none"> ▶ Ved brug af underdatabehandler indgår Compaya en databehandleraftale, der pålægger underdatabehandleren de samme databeskyttelsesforpligtelser, som databehandleren er pålagt. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af procedure for styring af underdatabehandlere.</p> <p>Vi har foretaget inspektion af en underdatabehandleraftale og set, at der fremgår de samme databeskyttelsesforpligtelser, som Compaya er pålagt.</p>	<p>Ingen afvigelser konstateret.</p>
<p>Godkendelse af underdatabehandlere</p> <ul style="list-style-type: none"> ▶ Udskiftning af underdatabehandlere følger den forudgående godkendelsesproces indgået med dataansvarlig. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har inspiceret, at der er udarbejdet en aftaleskabelon ved indgåelse af databehandleraftaler samt en procedure for styring af disse.</p> <p>Vi har foretaget inspektion af én stikprøve for en indgået databehandleraftale for henholdsvis CPSMS.dk og ProSMS.se/SMS.dk og set, at databehandleraftalerne omfatter bestemmelser vedrørende udskiftning af underdatabehandlere.</p> <p>Vi har på forespørgsel fået oplyst, at der i det seneste år ikke har været tilfælde, hvor databehandleren har foretaget ændringer i forhold til godkendte underdatabehandlere, hvorfor det ikke har været muligt at teste implementeringen af den indførte kontrol.</p>	<p>Ingen afvigelser konstateret.</p>

Artikel 28, stk. 2 og 4: Underdatabehandlere

Kontrolmål

- ▶ *At sikre, at underdatabehandleren er pålagt de samme databeskyttelsesforpligtelser, som databehandleren er pålagt af den dataansvarlige, ved indgåelse af en skriftlig kontrakt med tilhørende instruks.*
- ▶ *At sikre, at den dataansvarlige har givet en forudgående specifik eller generel skriftlig godkendelse af underdatabehandlere.*
- ▶ *At sikre, at underdatabehandleren kan stille de fornødne garantier til beskyttelse af personoplysningerne i overensstemmelse med kontrakten.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
<p>Tilsyn med underdatabehandlere</p> <ul style="list-style-type: none"> ▶ Compaya udfører tilsyn, herunder indhenter og gennemgår underdatabehandlers revisorerklæringer, certificeringer og lignende dokumenter. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af procedure for styring af underdatabehandlere hvor der fremgår, bestemmelser vedrørende indhentning og gennemgang af underdatabehandlers revisorerklæringer, certificeringer og lignende dokumenter.</p> <p>Vi har foretaget inspektion af dokumentation, som bekræfter, at der er foretaget gennemgang af erklæringer indhentet fra underdatabehandlere. Vi har ved forespørgsel fået oplyst, at en ISAE 3402 fra team.blue Denmark er fundet tilstrækkelig, idet der kun er tale om hosting.</p> <p>Vi har inspiceret ISAE 3402-erklæringen fra team.blue Denmark A/S for perioden 1. januar til 31. december 2023 samt ISAE 3000 fra Rackhosting ApS pr. 1. maj 2022 til 30. april 2023.</p>	<p>Ingen afvigelser konstateret.</p>

Artikel 28, stk. 3, litra b: Fortrolighed og lovbestemt tavshedspligt
Kontrolmål

- ▶ *At sikre, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
<p>Tavsheds- og fortrolighedsaftale med medarbejdere</p> <ul style="list-style-type: none"> ▶ Alle medarbejdere har underskrevet en ansættelseskontrakt, der indeholder en bestemmelse om fortroligheds- og tavshedspligt. ▶ Compaya indgår fortrolighedsaftaler med eksterne konsulenter med adgang til persondata. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af procedure for indgåelse af tavshedsaftale med medarbejdere.</p> <p>Vi har foretaget inspektion af én stikprøve for en medarbejder hvor det fremgår, at medarbejderen har underskrevet ansættelseskontrakt, der indeholder en bestemmelse om fortroligheds- og tavshedspligt.</p> <p>Vi har foretaget inspektion af én stikprøve for en konsulent og set, at konsulenten har underskrevet en fortrolighedsaftale.</p>	<p>Ingen afvigelser konstateret.</p>

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- ▶ At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.
- ▶ At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.
- ▶ At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.
- ▶ At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.
- ▶ At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.

Kontrolaktivitet	Test udført af BDO	Resultat af test
Risikovurdering <ul style="list-style-type: none"> ▶ Compaya har udarbejdet en risikovurdering i forhold til registreredes rettigheder og frihedsrettigheder. Compaya har udarbejdet og implementeret en procedure, der sikrer, at sikkerhedsforanstaltningerne revideres og ajourføres. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af risikovurderingen og set, at der er foretaget en vurdering af risici og konsekvenser i forhold til persondataforordningen.</p> <p>Vi har foretaget inspektion af årshjulet, der sikrer løbende svurdering og ajourføring af sikkerhedsforanstaltninger og inspiceret, at der er udført en halvårlig opdatering af risikovurderingen.</p>	Ingen afvigelser konstateret.
Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse <ul style="list-style-type: none"> ▶ Compaya har udarbejdet en beredskabsplan. ▶ Compaya har foretaget test af beredskabsplanen. 	<p>Vi har udført forespørgsel hos passende personale hos databehandleren.</p> <p>Vi har foretaget inspektion af beredskabsplanen og inspiceret, at beredskabsplanen omfatter en beskrivelse af blandt andet rolle og ansvar i beredskabsorganisationen, forudsætninger for aktivering samt plan for eskalering.</p> <p>Vi har inspiceret it-beredskabsplanen og observeret, at denne seneste er opdateret i januar 2024.</p> <p>Vi har inspiceret dokumentation for gennemført skrivebordstest af it-beredskabsplanen samt erfaringsopsamling med baggrund heri.</p>	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- ▶ *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- ▶ *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- ▶ *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- ▶ *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- ▶ *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Opbevaring af personoplysninger <ul style="list-style-type: none"> ▶ Personoplysninger i elektronisk form er kun tilgængelige for databehandlerens medarbejdere. ▶ Adgang til personoplysninger tildeles på baggrund af arbejdsbetinget behov/need-to-know principper. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af it-sikkerhedshåndbogen og procedure for adgang til personoplysninger. Vi har foretaget inspektion af dokumentation, som bekræfter, at kun autoriserede medarbejdere har adgang til personoplysninger.</p> <p>Vi har foretaget inspektion af procedure for adgang til personoplysninger og hvor det fremgår, at adgang til personoplysninger tildeles på baggrund af arbejdsbetinget behov/need-to-know principper.</p> <p>Vi har foretaget inspektion af databehandlerens brugeradgang, hvor det fremgår at medarbejdernes adgang til personoplysninger tildeles på baggrund af arbejdsbetinget behov.</p>	Ingen afvigelser konstateret.
Fysisk adgangskontrol <ul style="list-style-type: none"> ▶ Der er etableret fysiske adgangskontroller i forhold til Compaya's kontorer og lokaler. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af it-sikkerhedshåndbogen og procedure for fysiske adgangskontroller i forhold til databehandlerens kontorer og lokaler.</p> <p>Vi har foretaget inspektion af liste over nøgle og brikker, som er udleveret til medarbejdere i overensstemmelse med databehandlerens procedure.</p> <p>Vi har observeret, at databehandleren har en alarm ved døren.</p>	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- ▶ *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- ▶ *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- ▶ *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- ▶ *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- ▶ *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Logisk adgangskontrol <ul style="list-style-type: none"> ▶ Compaya har implementeret procedure for brugeradministration, der sikrer, at brugeroprettelser og -nedlæggelser følger en styret proces, og at alle brugeroprettelser er autoriseret. ▶ Der foretages løbende gennemgang af brugere og brugerrettigheder. ▶ Compaya's krav til adgangskoder følges af alle medarbejdere samt eksterne konsulenter. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af procedure for brugeradministration hvoraf der fremgår retningslinjer for oprettelse og nedlæggelse af brugere.</p> <p>Vi har foretaget inspektion af it-sikkerhedshåndbogen, hvor det fremgår, at der ifølge denne mindst en gang om året skal foretages en gennemgang af brugeres rettigheder.</p> <p>Vi har foretaget inspektion af dokumentation, som bekræfter, at Compaya har gennemgået brugere og brugerrettigheder i april 2024 i overensstemmelse med årshjulet.</p> <p>Vi har foretaget inspektion af dokumentation, som bekræfter, at krav til adgangskoder følges af alle medarbejdere samt eksterne konsulenter.</p>	Ingen afvigelser konstateret.
Fjernarbejdspladser og fjernadgang til systemer og data <ul style="list-style-type: none"> ▶ Fjernadgang til Compaya's systemer og data sker via en krypteret VPN-forbindelse. ▶ Der anvendes en sikker forbindelse mellem Compaya og underleverandør. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af databehandlerens IT-sikkerhedshåndbog, hvoraf det fremgår at VPN-forbindelsen er krypteret.</p> <p>Vi har foretaget inspektion af dokumentation, som bekræfter, at der anvendes VPN-forbindelse med kryptering.</p>	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- ▶ At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.
- ▶ At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.
- ▶ At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.
- ▶ At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.
- ▶ At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har foretaget inspektion af dokumentation, som bekræfter, at der anvendes en sikker forbindelse mellem Compaya og underdatabehandleren.	
Netværkssikkerhed <ul style="list-style-type: none"> ▶ Compaya's kontornetværk er segmenteret. ▶ Compaya anvender kendte netværksteknologier og mekanismer til overvågning af kontorets netværk. ▶ Der er begrænset antal medarbejdere, der har adgang til at foretage ændringer i Firewall for kontorets netværk. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af databehandlerens procedure for styring og opdeling af netværkssikkerhed.</p> <p>Vi har foretaget inspektion af dokumentation for netværkssegmentering.</p> <p>Vi har foretaget inspektion af dokumentation, som bekræfter, at der anvendes Zabbix til overvågning af kontorets netværk.</p> <p>Vi har foretaget inspektion af dokumentation, som bekræfter, at det kun er de autoriserede medarbejdere, der har adgang til at foretage ændringer i Compaya's lokale netværks Firewall.</p>	Ingen afvigelser konstateret.
Antivirusprogram <ul style="list-style-type: none"> ▶ Der er installeret antivirus-software på alle arbejdsstationer. ▶ Medarbejderens PC'er er sat op til automatiske opdateringer (Patch Management). 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af databehandlerens procedure for beskyttelse mod virus og malware mv.</p> <p>Vi har ved en stikprøve foretaget inspektion af dokumentation for installation af antivirus for seneste tiltrådte medarbejders PC.</p>	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- ▶ At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.
- ▶ At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.
- ▶ At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.
- ▶ At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.
- ▶ At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har foretaget inspektion af dokumentation, som bekræfter, at der foretages automatiske opdateringer af medarbejderes PC'er.	
Sikkerhedskopiering og retablering af data <ul style="list-style-type: none"> ▶ Compaya har udarbejdet og implementeret procedure for backup. ▶ Der foretages dagligt backup af systemer og data. ▶ Der udføres løbende, dog mindst en gang om året, en restore-test af backup. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af Compaya's backuppolitik og procedure for backup, herunder verificering og reetablering af backup.</p> <p>Vi har foretaget inspektion af dokumentation, som bekræfter, at der foretages dagligt backup af systemer og data.</p> <p>Vi har inspiceret dokumentation for udført restore-test af backup foretaget i april 2024.</p>	Ingen afvigelser konstateret.
Logning af anvendelse af personoplysninger <ul style="list-style-type: none"> ▶ Alle succesfulde og mislykkede adgangsforsøg til SMS-systemerne og data logges. ▶ Logfiler er kun tilgængelige for drifts- og supportmedarbejdere. ▶ Logdata med persondata slettes efter 6 måneder. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af dokumentation, som bekræfter, at alle succesfulde og mislykkede adgangsforsøg til SMS-systemer (CPSMS.dk, ProSMS.se/SMS.dk og data logges.</p> <p>Vi har foretaget inspektion af dokumentation, som bekræfter, at logfiler kun er tilgængelige for drifts- og supportmedarbejdere.</p>	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrolmål

- ▶ At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.
- ▶ At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.
- ▶ At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.
- ▶ At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.
- ▶ At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har foretaget inspektion af dokumentation, som bekræfter, at logdata med persondata slettes efter 6 måneder.	
Overvågning <ul style="list-style-type: none"> ▶ Compaya har etableret et overvågningssystem til overvågning af produktionsmiljø, herunder opetid, ydeevne og kapacitet. ▶ Compaya notificeres om alarmer og følger op herpå. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af it-sikkerhedshåndbogen, hvori procedure for overvågning er beskrevet.</p> <p>Vi har foretaget inspektion af dokumentation vedrørende overvågning og observeret, at der anvendes Zabbix til overvågning af produktionsmiljø, herunder opetid, ydeevne og kapacitet.</p> <p>Vi har foretaget inspektion af dokumentation, som bekræfter, at der modtages meddelelser i form af e-mails fra Zabbix med identificerede alarmer.</p>	Ingen afvigelser konstateret.
Retningslinjer for fjernelse eller destruktion af it-udstyr <ul style="list-style-type: none"> ▶ Persondata er fjernet/overskrevet i forbindelse med PC'er bortskaffes eller genbruges. ▶ Compaya bortskaffer it-udstyr ved fysisk destruktion af databærende medier. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af it-sikkerhedshåndbogen, procedure for reparation og bortskaffelse af it-udstyr.</p> <p>Vi har fået oplyst, at der ikke har været tilfælde, hvor Compaya har skullet bortskaffe it-udstyr ved fysisk destruktion, hvorfor det ikke har været muligt at teste implementeringen af de indførte kontroller.</p>	Ingen afvigelser konstateret.

Artikel 25: Databeskyttelse gennem design og standardindstillinger		
Kontrolmål ► At sikre, at databehandleren gennemfører databeskyttelse gennem design og standardindstillinger.		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Tekniske og organisatoriske foranstaltninger vedrørende udvikling <ul style="list-style-type: none"> ► Compaya har udarbejdet procedure for udviklingsprocessen, der sikrer Privacy by Design og Privacy by Default. ► Compaya instruerer medarbejderne om Privacy by Design og Privacy by Default. ► Udvikling og test udføres i udviklingsmiljøer, som er adskilte fra produktionssystemer. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af Compaya's procedure for udviklingsprocessen, der sikrer databeskyttelse gennem design og standardindstillinger.</p> <p>Vi har foretaget inspektion af dokumentation, som bekræfter, at Compaya har instrueret medarbejderne om kravene til Privacy by Design og Privacy by Default.</p> <p>Vi har foretaget inspektion af netværkstopologi, som bekræfter, at udviklings-, test- og produktionsmiljøet er adskilte.</p> <p>Vi har foretaget inspektion af dokumentation, som viser, at udviklingsopgavers løbende fremdrift er dokumenteret i Compaya's opgavestyringssystem Pivotal Tracker.</p>	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra g: Sletning og tilbagelevering af personoplysninger

Kontrolmål

- ▶ At sikre, at databehandleren kan slette og tilbagelevere personoplysninger, efter at tjenesten vedrørende behandlingen er ophørt, i henhold til instruks fra den dataansvarlige.

Kontrolaktivitet	Test udført af BDO	Resultat af test
<p>Sletning af personoplysninger</p> <ul style="list-style-type: none"> ▶ Compaya sletter den dataansvarliges personoplysninger efter instruks, ved ophør af hovedaftalen. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af procedure for behandling af kunde-data hvori er beskrevet bestemmelser vedr. sletning af personoplysninger.</p> <p>Vi har foretaget inspektion af dokumentation, som bekræfter, at der er implementeret tekniske foranstaltninger, som muliggør sletning af persondata i SMS-systemer (CPSMS.dk, ProSMS.se/SMS.dk.)</p> <p>Vi har på forespørgsel fået oplyst, at der ikke har været henvendelser fra den dataansvarlige vedrørende sletning af personoplysninger, hvorfor det ikke har være muligt at teste implementeringen af den indførte kontrol.</p>	<p>Ingen afvigelser konstateret.</p>

Artikel 28, stk. 3, litra e, f og h: Bistand til den dataansvarlige

Kontrolmål

- ▶ *At sikre, at databehandleren kan bistå den dataansvarlige med opfyldelse af de registreredes rettigheder.*
- ▶ *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til behandlingssikkerhed (artikel 32), brud på persondatasikkerheden (artikel 33-34) og konsekvensanalyser (artikel 35-36).*
- ▶ *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til revision og inspektion.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Bistand - de registreredes rettigheder <ul style="list-style-type: none"> ▶ Compaya kan bistå den dataansvarlige med opfyldelse af de registreredes rettigheder. ▶ Compaya kan give indsigt i alle oplysninger, der er registreret hos databehandler. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af procedure for bistand til den dataansvarlige, hvoraf der fremgår bestemmelser vedrørende bistand med opfyldelse af de registreredes rettigheder.</p> <p>Vi har foretaget inspektion af skabelon for databehandlersaftale samt én stikprøve for en underskrevet databehandlersaftale for henholdsvis CPSMS.dk, ProSMS.se/SMS.dk og, at der heraf fremgår, at databehandleren skal bistå den dataansvarlige med opfyldelse af de registreredes rettigheder.</p> <p>Vi har på forespørgsel fået oplyst, at der ikke har været tilfælde vedrørende håndtering af bistand til den dataansvarlige, hvorfor det ikke har været muligt at teste implementeringen af de indførte kontroller.</p> <p>Vi har foretaget inspektion, at databehandleren kan give indsigt i alle oplysninger, der er registreret hos databehandler.</p>	Ingen afvigelser konstateret.
Bistand - revision og inspektion <ul style="list-style-type: none"> ▶ Compaya udarbejder årligt en ISAE 3000-erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger, rettet mod behandling og beskyttelse af personoplysninger. ▶ Compaya kan bistå den dataansvarlige ved fysisk tilsyn. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af skabelon for databehandlersaftale, at der heraf fremgår, at databehandleren skal udarbejde en årlig ISAE 3000-erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger, rettet mod behandling og beskyttelse af personoplysninger.</p> <p>Vi har udarbejdet nærværende ISAE 3000-erklæring til brug for databehandlerens forpligtelser i denne relation.</p>	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra e, f og h: Bistand til den dataansvarlige

Kontrolmål

- ▶ At sikre, at databehandleren kan bistå den dataansvarlige med opfyldelse af de registreredes rettigheder.
- ▶ At sikre, at databehandleren kan bistå den dataansvarlige i forhold til behandlingssikkerhed (artikel 32), brud på persondatasikkerheden (artikel 33-34) og konsekvensanalyser (artikel 35-36).
- ▶ At sikre, at databehandleren kan bistå den dataansvarlige i forhold til revision og inspektion.

Kontrolaktivitet	Test udført af BDO	Resultat af test
	<p>Vi har foretaget inspektion af procedure for bistand til den dataansvarlige, at der heri fremgår bestemmelser vedrørende bistand i forhold til revision og inspektion.</p> <p>Vi har foretaget inspektion af, det af databehandleraftalen fremgår, at databehandleren har forpligtet sig til at bistå den dataansvarlige ved fysisk tilsyn.</p> <p>Vi har på forespørgsel fået oplyst, at der ikke har været tilfælde vedrørende bistand ved fysisk tilsyn, hvorfor det ikke har været muligt at teste implementeringen af den indførte kontrol.</p>	
<p>Bistand - særlige krav i forordningen</p> <ul style="list-style-type: none"> ▶ Compaya kan bistå den dataansvarlige i forbindelse med opfyldelse af behandlingssikkerhed (artikel 32), anmeldelse af brud på persondatasikkerheden til de dataansvarlige (artikel 33), konsekvensanalyse vedrørende databeskyttelse (artikel 35), forudgående høring (artikel 36). 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af følgende dokumentation:</p> <ul style="list-style-type: none"> • Informationssikkerhedspolitikken • Persondatapolitikken for hver af SMS-systemerne • Procedure for håndtering af brud på persondatasikkerhed • Databehandlerens databrudslog • Procedure for adgang til personoplysninger i SMS-systemerne • Procedure for behandling af kundedata i SMS-systemerne. <p>Vi har foretaget inspektion af procedure for bistand til den dataansvarlige, hvor det fremgår bestemmelser i forhold til overholdelse af særlige krav i forordningen, herunder anmeldelse af sikkerhedsbrud, konsekvensanalyser og forudgående høringer fra tilsynsmyndighederne.</p> <p>Vi har foretaget inspektion af skabelon for databehandlerens databehandleraftale samt de seneste indgåede databehandleraftaler, hvoraf det fremgår, at databehandleren forpligter sig til at bistå de dataansvarlige med disses forpligtelser i forhold til anmeldelse</p>	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra e, f og h: Bistand til den dataansvarlige

Kontrolmål

- ▶ *At sikre, at databehandleren kan bistå den dataansvarlige med opfyldelse af de registreredes rettigheder.*
- ▶ *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til behandlingssikkerhed (artikel 32), brud på persondatasikkerheden (artikel 33-34) og konsekvensanalyser (artikel 35-36).*
- ▶ *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til revision og inspektion.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	<p>af sikkerhedsbrud, konsekvensanalyser og forudgående høringer fra tilsynsmyndighederne.</p> <p>Vi har på forespørgsel fået oplyst, at der ikke har været tilfælde vedrørende håndtering af bistand til den dataansvarlige vedrørende særlige krav i forordningen i overensstemmelse med artikel 32-36, hvorfor det ikke har været muligt at teste implementeringen af de indførte procedurer.</p>	

Artikel 30, stk. 2, 3 og 4: Fortegnelse over kategorier af behandlingsaktiviteter

Kontrolmål

- ▶ *At sikre, at databehandleren udarbejder en skriftlig fortegnelse over alle kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige.*
- ▶ *At sikre, at databehandleren opbevarer fortegnelsen skriftligt, herunder elektronisk.*
- ▶ *At sikre, at databehandleren kan stille fortegnelsen til rådighed for tilsynsmyndigheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
<p>Fortegnelse over kategorier af behandlingsaktiviteter</p> <ul style="list-style-type: none"> ▶ Compaya har udarbejdet en fortegnelse over behandlingsaktiviteter som databehandler. ▶ Fortegnelsen opbevares elektronisk. ▶ Fortegnelsen opdateres løbende og minimum en gang årligt under det årlige review. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af, at Compaya har udarbejdet fortegnelser over behandlingsaktiviteter. Vi har foretaget inspektion af denne fortegnelse.</p> <p>Vi har observeret, at fortegnelsen opbevares elektronisk.</p> <p>Vi har foretaget inspektion af årshjulet og observeret, at opdateringen af fortegnelsen sker løbende og som minimum en gang årlig, hvilket fremgår af årshjulet.</p>	<p>Ingen afvigelser konstateret.</p>

Artikel 33, stk. 2: Underretning om brud på persondatasikkerheden

Kontrolmål

- ▶ *At sikre, at databehandleren uden unødigt forsinkelse underretter den dataansvarlige om brud på persondatasikkerheden.*
- ▶ *At sikre, at den dataansvarlige underrettes om alle nødvendige oplysninger, så bruddet kan vurderes med henblik på anmeldelse til tilsynsmyndigheden og underretning til den registrerede.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
<p>Underretning om brud på persondatasikkerheden</p> <ul style="list-style-type: none"> ▶ Compaya har udarbejdet en procedure for håndtering af brud på persondatasikkerhed. ▶ Compaya har udarbejdet og implementeret en procedure for underretning af den dataansvarlige ved brud på persondatasikkerhed. ▶ Compaya registrerer brud på persondatasikkerheden i databrudsloggen. 	<p>Vi har udført forespørgsel hos passende personale hos Compaya.</p> <p>Vi har foretaget inspektion af procedure for håndtering af brud på persondatasikkerhed, hvor der fremgår, retningslinjer for registrering af brud på persondatasikkerhed.</p> <p>Vi har foretaget inspektion af procedure for underretning af den dataansvarlige ved brud på persondatasikkerhed, hvor det fremgår, at den dataansvarlige underrettes uden unødigt forsinkelse, efter at Compaya er blevet opmærksom på, at der er sket brud på persondatasikkerheden.</p> <p>Vi har foretaget inspektion af et skema som udfyldes ved brud på persondatasikkerheden.</p> <p>Vi har på forespørgsel fået oplyst, at der ikke har været brud på persondatasikkerheden, hvorfor det ikke har været muligt at teste implementeringen af de indførte kontroller.</p>	<p>Ingen afvigelser konstateret.</p>

**BDO STATSATORISERET
REVISIONSAKTIESELSKAB**

**VESTRE RINGGADE 28
8000 AARHUS C**

www.bdo.dk

BDO Statsautoriseret revisionsaktieselskab, danskejet rådgivnings- og revisionsvirksomhed, er medlem af BDO International Limited - et UK-baseret selskab med begrænset hæftelse - og del af det internationale BDO-netværk bestående af uafhængige medlems-firmaer. BDO er varemærke for både BDO-netværket og for alle BDO medlemsfirmaerne. BDO i Danmark beskæftiger mere end 1.700 medarbejdere, mens det verdensomspændende BDO-netværk har over 115.000 medarbejdere i 166 lande.

*Copyright - BDO Statsautoriseret revisionsaktieselskab,
cvr.nr. 20 22 26 70.*

