

April 2024

CompuSoft A/S

ISAE 3000 TYPE 1 ERKLÆRING

CVR 21774774

Uafhængig revisors ISAE 3000 erklæring om informationssikkerhed og foranstaltninger i henhold til databehandlersaftale med dataansvarlige, pr. 22. april 2024.

Beierholm
Statsautoriseret Revisionspartnerselskab
Tangen 9
8200 Aarhus N
CVR 32 89 54 68
Tlf.: +45 87 32 57 00

www.beierholm.dk



Erklæringsopbygning

Kapitel 1:

Ledelseserklæring.

Kapitel 2:

Uafhængig revisors ISAE 3000 erklæring om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med CompuSoft A/S' kunder.

Kapitel 3:

Beskrivelse af behandling.

Kapitel 4:

Kontrolmål, kontrolaktivitet, test og resultat heraf.


Ledelseserklæring

CompuSoft A/S' behandler personoplysninger på vegne af kunder (dataansvarlige) i henhold til indgåede databehandleraftaler.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt CompuSoft A/S' ydelser som beskrevet i kapitel 3, 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' forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") er overholdt.

CompuSoft A/S bekræfter, at:

- 1) Den medfølgende beskrivelse giver en retvisende beskrivelse af CompuSoft A/S' ydelser, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen pr. 22. april 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:
 - a) Redegør for, hvordan ydelserne var udformet og implementeret, herunder redegør for:
 - i) De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger.
 - ii) 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.
 - iii) De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige.
 - iv) 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.
 - v) 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.
 - vi) De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registre-rede.
 - vii) 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.
 - viii) Kontroller, som vi med henvisning til CompuSoft A/S' ydelsers afgrænsning har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen.
 - ix) Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger.

- 
- b) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne 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 behandlingen, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.
- 2) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. 22. april 2024. Kriterierne anvendt for at give denne udtalelse var, at:
- a) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret,
- b) De identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål.
- 3) 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.

Søndersø, 30. april 2024

Thomas Traberg-Larsen
Direktør
CompuSoft A/S

Uafhængig revisors ISAE 3000 erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med CompuSoft A/S' kunder

Til CompuSoft A/S

Omfang

Vi har fået som opgave at afgive erklæring om CompuSoft A/S' beskrivelse af ydelserne jf. kapitel 3 i henhold til databehandleraftaler med CompuSoft A/S' kunder pr. 22. april 2024 og om udformningen og implementeringen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med høj grad af sikkerhed.

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

Beskrivelsen i kapitel 3, afsnittet om komplementerende kontroller hos dataansvarlige, angiver at visse kontrolmål, kun kan opnås hvis komplementerende kontroller hos dataansvarlige er passende designet og operationelt effektive sammen med relaterede kontroller hos CompuSoft A/S.

Vores handlinger har ikke omfattet kontrolaktiviteter udført af dataansvarlige, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos kunderne.

CompuSoft A/S' ansvar

CompuSoft A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse jf. kapitel 3, 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.

Beierholms uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR – danske revisors retningslinjer for revisors etiske adfærd (Ethiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

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

Revisors ansvar

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

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

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af sit system samt for kontrollernes udformning. De valgte handlinger afhænger af 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 mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i kapitel 3.

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

Begrænsninger i kontroller hos CompuSoft A/S

CompuSoft 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 medieplatformen, 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. Det er vores opfattelse,

- a) at beskrivelsen af ydelserne, således som disse var udformet og implementeret pr. 22. april 2024, i alle væsentlige henseender er retvisende, og
- b) at kontrollerne, som knyttede sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet og implementeret pr. 22. april 2024

Beskrivelse af test kontroller

De specifikke kontroller, der er testet, samt arten, den tidsmæssige placering og resultater af disse test fremgår af kapitel 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller under kapital 4 er udelukkende tiltænkt CompuSoft A/S' kunder der har anvendt ydelserne som beskrevet i kapitel 3 og som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

Aarhus, 30. april 2024

Beierholm

Statsautoriseret Revisionspartnerselskab

Kim Larsen
Statsautoriseret revisor

Jens Theodor Saugbjerg
IT-auditor

Beskrivelse af behandling.

Formålene med CompuSoft A/S' behandling af persondata er at give dataansvarliges personale adgang til et system, der kan hjælpe dem med at håndtere kundens bookinger og billetter samt i denne forbindelse opkræve betalinger samt udstede fakturaer, yde teknisk support, fejlfinding og vedligeholdelse af Systemet, beskytte imod svig, uretmæssige handlinger og sikkerhedsbrud.

Om CompuSoft A/S

CompuSoft A/S er førende inden for bookingsystemer og billetløsninger til campingpladser, feriecentre og turismevirksomheder i Skandinavien. Vi tilbyder omnichannel commerce-løsninger, der omfatter e-handelsplatforme, bookingsystemer, gæsteapps og adgangskontrol. Vores ekspertise inden for digitalisering og omnichannel-strategi hjælper med at optimere virksomhedsdrift og gæsteservice. Vi betjener over 600 campingpladser, feriecentre og attraktioner dagligt.

Karakteren af behandlingen

CompuSoft A/S' behandling drejer sig primært om indsamling, registrering, organisering, strukturering, opbevaring, tilpasning eller ændring af personoplysninger i overensstemmelse med den dataansvarliges instruktioner.

Kategorier af registrerede personer omfattet af databehandleraftalerne:

- Kunder, potentielle kunder og gæster hos dataansvarlige
- Medarbejdere hos dataansvarlige (login informationer)

Behandlingen omfatter følgende typer af almindelige personoplysninger:

- **Kunder, potentielle kunder og gæster:** Navn, adresse, postnummer, by, nationalitet, telefonnummer, kortoplysninger, korrespondance, indhold i fritekstfelter, købte produkter samt e-mailadresse. Herudover registreres evt. opholdsperiode, antal personer, alder og køn.
- **Medarbejdere:** Navn, adresse, telefonnummer og e-mail.

Behandlingen omfatter følgende typer af særlige kategorier af personoplysninger:

- **CPR-nummer:** Kan behandles i særlige tilfælde, og udelukkende når dataansvarlig er en kommune eller statslig organisation og kun i det omfang det er nødvendigt for dataansvarlige af hensyn til opkrævning af betalinger.

Informationssikkerhedsmiljøet

Arbejdet med informationssikkerhed i CompuSoft A/S tager afsæt i god praksis for it-sikkerhed og er inspireret af ISO27001 standarden, som er baseret på en risikobaseret tilgang til styring af informationssikkerhed.

CompuSoft A/S har følgende overordnede målsætning for informationssikkerhed:

- Sikkerhedsniveauet skal fastlægges ud fra en risikobaseret tilgang, som balancerer sikkerhedshensyn og efterlevelse af databeskyttelseslovgivningen med forretningshensyn.
- Der arbejdes professionelt og struktureret med informationssikkerhed med inspiration fra ISO27001 standarden, som ramme for informationssikkerhedsledelse og - styring.
- Alle medarbejdere i CompuSoft A/S skal være bevidste om, at de spiller en vigtig og aktiv rolle i forhold til selskabets samlede informationssikkerhed. De skal kende og efterleve regler og retningslinjer for informationssikkerhed, som er relevante i deres daglige arbejde og være engageret i CompuSoft A/S' uddannelses- og træningsaktiviteter på området.

Praktiske tiltag

CompuSoft A/S opretholder en række organisatoriske og tekniske foranstaltninger for at sikre de personoplysninger der behandles i rammen af databehandleraftalerne.

Disse foranstaltninger omfatter bl.a.:

- Løbende sårbarhedsscanninger.
- Systematisk patching og opdatering af software.
- Monitorering af kritiske systemer, som leverer notifikationer hvis et eller flere systemer ikke agerer som forventet.
- Netværksovervågning.
- Logning af netværksaktivitet.
- Uafhængige backupløsninger.
- Fysisk sikkerhed og overvågning af datacentre.
- Redundante uafhængige nødstrømssystemer.
- Kryptering.
- Security incident management (nedbrudsprocedurer).
- Adskillelse af konto og rettigheder.

Kontrolforanstaltninger

CompuSoft A/S opretholder desuden en række specifikke kontrolforanstaltninger der skal sikre at der opretholdes et passende sikkerhedsniveau i systemerne, herunder:

Instruktion af medarbejdere:

Det sikres at ansatte og eventuelle samarbejdspartnere til stadighed er bekendt med og har tilstrækkelig uddannelse og instruktion om databehandlingens formål, politikker, arbejdsgange og om deres tavshedspligt.

Adgangsstyring og administration af brugeradgang:

Kun medarbejdere, som har et arbejdsbetinget behov for at behandle personoplysninger må være oprettet som brugere med adgang til dataansvarliges personoplysninger. Autorisationer (og herunder adgange) for brugere, der ikke længere har et arbejdsbetinget behov for autorisation annulleres uden ophold.

Kontrol med afviste adgangsforsøg

Med udgangspunkt i en risikobaseret tilgang foretages der registrering af afviste adgangsforsøg og blokeres for yderligere forsøg efter fastlagte antal på hinanden følgende afviste adgangsforsøg.

Derudover opretholdes procedurer, som sikrer rettidig opfølgning på alle afviste adgangsforsøg, hvor opfølgning er nødvendig for at forhindre brud på persondatasikkerheden og skadevirkninger for registrerede personer.

Ændringshåndtering

Der er implementeret formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering.

Eksterne kommunikationsforbindelser

Der er implementeret tekniske foranstaltninger til at beskytte systemer og netværk samt til at begrænse risikoen for uautoriseret adgang og/eller installering af skadelig kode.

I det omfang det er et krav i medfør af gældende lovgivning, god databehandlingsskik eller i øvrigt er omfattet af hovedaftalen anvendes tidssvarende krypteringsteknologier og andre tilsvarende foranstaltninger.

Der henvises i øvrigt til afsnit 4, hvor de konkrete kontrolaktiviteter er beskrevet.

Komplementerende kontroller hos de dataansvarlige

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

Den dataansvarlige har følgende forpligtelser:

- Dataansvarlig skal løbende sikre, at egen brugeradgang er ajourført, og at alle brugere er bekendt med den adgang, som systemet potentielt kan give til personoplysninger.
- Der skal tages stilling til og testes nye versioner af løsninger i forbindelse med implementering (ændringsstyring).
- Der skal udføres GDPR-oprydningskørsler for at slette forældede eller irrelevante personoplysninger fra de systemer, der tilbydes.
- Det er vigtigt at holde sig opdateret ved at følge nyhedsbreve og informationsbulletiner, der udsendes af CompuSoft A/S.
- Det er også vigtigt at holde sig ajour med CompuSoft's driftsinformationer, som kan tilgås via CompuSoft Helpdesk Manager.
- Endelig skal der tages stilling til, om instruksen er hensigtsmæssig i forhold til den indgåede databehandleraftale.

KAPITEL 4:

Kontrolmål, kontrolaktivitet, test og resultat heraf

KONTROLMÅL A:

Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.

CompuSoft A/S' kontroller	Revisors test af kontroller	Resultat af test
<p>A.1 Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foretages når der foreligger en instruks.</p> <p>Vi har observeret, at der er implementeret tekniske foranstaltninger der understøtter proceduren.</p> <p>Vi har forespurgt, om de involverede nøglepersoner er bekendte med procedurerne.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>A.2 Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.</p>	<p>Vi har forespurgt, om ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.</p> <p>Vi har via stikprøver inspiceret, at behandlingen af personoplysninger foregår i overensstemmelse med instruks.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>A.3 Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandleren mening er i strid med databeskyttelsesforordningen eller medlemsstaternes nationale ret.</p>	<p>Vi har inspiceret, at der foreligger procedurer, der sikrer, at dataansvarlige underrettes i tilfælde af at databehandler vurderer, at instrukser for behandling af personoplysninger er i strid med databeskyttelsesforordningen eller anden lovgivning.</p> <p>Vi har forespurgt, om ledelsen har sikret at nuværende behandlinger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

KONTROLMÅL B:

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

CompuSoft A/S' kontroller	Revisors test af kontroller	Resultat af test
<p>B.1 Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger.</p> <p>Vi har inspiceret, at procedurerne indeholder krav om minimum årlig vurdering.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>B.2 Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.</p>	<p>Vi har inspiceret, at der, som minimum årligt, udføres en risikovurdering af medieplatformen og databehandlingen.</p> <p>Vi har inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger.</p> <p>Vi har inspiceret, at databehandler har implementeret de tekniske sikkerhedsforanstaltninger, som er vurderet passende på baggrund af risikovurderingen.</p> <p>Vi har via stikprøver på indgåede databehandleraftaler inspiceret, at der er etableret de aftalte sikringsforanstaltninger.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>B.3 Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.</p>	<p>Vi har inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus software.</p> <p>Vi har inspiceret, at antivirus software er konfigureret til automatisk scanning af systemer og databaser.</p> <p>Vi har inspiceret, at antivirus software er opdateret.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>B.4 Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.</p>	<p>Vi har inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall.</p> <p>Vi har inspiceret, at firewall er konfigureret i henhold til intern politik herfor.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

<p>B.5 Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.</p>	<p>Vi har inspiceret tilgængelig netværksdokumentation, og påset at netværk er behørigt segmenteret.</p> <p>Vi har forespurgt hvorvidt det sikres, at interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger, samt hvorvidt det sikres at der er segmentering mellem databaser hvor der behandles data fra forskellige dataansvarlige.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>B.6 Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.</p>	<p>Vi har inspiceret, at adgang til systemer og databaser med personoplysninger, er begrænset til brugere med arbejdsbetinget behov herfor.</p> <p>Vi har inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>B.7 Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.</p>	<p>Vi har inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.</p> <p>Vi har observeret, at der modtages alarmer og påset disse behandles jævnfør formaliserede processer.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>B.8 Der anvendes effektiv kryptering ved transmission af personoplysninger via internettet.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer at transmission og opbevaring af personoplysninger, foregår krypteret.</p> <p>Vi har inspiceret, at der anvendes effektiv kryptering ved transmission af oplysninger, herunder anvendelse af FTP-S.</p> <p>Vi har inspiceret, at der er aktive certifikater på alle relevante services.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>B.9 Der er etableret logning i systemer, databaser og netværk. Logningen omfatter bl.a.:</p> <ul style="list-style-type: none"> • Tekniske logs af hændelser på tværs af systemer og platforme. • Sikkerhedshændelser omfattende bl.a.: <ul style="list-style-type: none"> ○ Brugerlogins på systemer og databaser ○ Fejlede loginforsøg ○ Installation af software 	<p>Vi har inspiceret, at der er etableret logning i systemer, databaser og netværk der kan kontrolleres.</p> <p>Vi har inspiceret, at der modtages notifikationer når udpegede sikkerhedshændelser indtræffer.</p> <p>Vi har stikprøvevist inspiceret, at logfiler har det forventede indhold og forhold til opsætningen.</p> <p>Vi har forespurgt, om der er procedurer for gennemgang af logoplysninger.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

<p>B.10 Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form.</p> <p>Anvendelse af ikke-anonymiseret persondata sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.</p>	<p>Vi har forespurgt, at om foreligger formaliserede procedurer for anvendelse af persondata i testmiljøer, der sikrer at data altid skal være i anonymiseret form eller anvendes i henhold til gyldig instruks fra dataansvarlig.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>B.11 De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.</p>	<p>Vi har inspiceret, at der er konfigureret løbende sårbarhedsscanninger af systemer og netværk.</p> <p>Vi har forespurgt, om der foretages penetrationstest af systemer og netværk.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>B.12 Ændringer til systemsoftware følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder kritiske opdateringer.</p>	<p>Vi har inspiceret, at der er etableret et fast system for udvikling og ændringer i systemer, databaser og netværk, der sikrer at systemudvikling og vedligeholdelse foregår styret.</p> <p>Vi har inspiceret, at systemer og databaser er opdateret med seneste relevante opdateringer og patches.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>B.13 Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugerens adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer for tildeling, revurdering og afbrydelse af brugerens adgang til systemer og databaser, som anvendes til behandling af personoplysninger.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>B.14 Ekstern adgang til systemer og databaser, hvori der sker behandling af personoplysninger, sker som minimum ved anvendelse af to-faktor autentifikation.</p>	<p>Vi har forespurgt, om der er implementeret to-faktor autentifikation ved ekstern adgang til systemer og databaser.</p> <p>Vi har observeret, at der foretages to-faktor autentifikation, ved ekstern adgang til systemer og databaser.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>B.15 Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.</p>	<p>Vi har inspiceret, at der er etableret passende fysisk adgangssikkerhed og påset, at der føres kontrol over medarbejderes adgange, samt at der kun er fysisk adgang til servere, for særlig autoriserede medarbejdere.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

KONTROLMÅL C:

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

CompuSoft A/S' kontroller	Revisors test af kontroller	Resultat af test
<p>C.1 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.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om IT-sikkerhedspolitikken skal opdateres.</p>	<p>Vi har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år.</p> <p>Vi har inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>C.2 Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.</p>	<p>Vi har forespurgt hvorvidt ledelsen sikrer, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.</p> <p>Vi har inspiceret informationssikkerhedspolitikken og påset, at der ikke er uoverensstemmelser med kravene til sikringsforanstaltninger og behandlingssikkerhed i indgåede databehandleraftaler.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>C.3 Der udføres i relevant omfang efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.</p>	<p>Vi har forespurgt, hvorvidt der udføres relevant efterprøvning af medarbejdere i forbindelse med ansættelse.</p> <p>Vi har inspiceret, at der er formaliserede procedurer, der sikrer efterprøvning af medarbejdere i forbindelse med ansættelsen.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>C.4 Ved ansættelse underskriver medarbejdere en ansættelseskontrakt med krav om tavshedspligt.</p> <p>Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.</p>	<p>Vi har inspiceret standardansættelseskontrakterne, og kontrolleret at disse indeholder bestemmelser om tavshedspligt.</p> <p>Vi har inspiceret, at der er formaliserede procedurer, der sikrer at nye medarbejdere introduceres til gældende politikker og procedurer for databehandling og behandlingssikkerhed.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>C.5 Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.</p>	<p>Vi har inspiceret, at der foreligger en formaliseret procedure, der sikrer, at fratrådte medarbejders rettigheder inaktiveres eller ophører fra fratrædelse, og at udleverede aktiver inddrages.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

<p>C.6 Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelsen af tavshedspligten.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>C.7 Der gennemføres løbende awareness-aktiviteter, og orientering af databehandlerens medarbejdere om IT-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.</p>	<p>Vi har forespurgt, om det tilsikres at medarbejdere løbende holdes orienteret om IT-sikkerhed og relevante procedurer.</p> <p>Vi har observeret, at der udsendes regelmæssige mails med informationer om GDPR.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

KONTROLMÅL D:

Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.

CompuSoft A/S' kontroller	Revisors test af kontroller	Resultat af test
<p>D.1 Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at opbevaring og sletning af personoplysninger foregår i overensstemmelse med aftalen indgået med den dataansvarlige.</p> <p>Vi har inspiceret, at procedurerne er opdateret.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>D.2 Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder:</p> <ul style="list-style-type: none"> • Data kan opbevares i hele aftalens løbetid. 	<p>Vi har inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>D.3 Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige:</p> <ul style="list-style-type: none"> • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning 	<p>Vi har inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger.</p>	<p>Der var på revisionsdagen ikke nyligt opførte behandlinger, hvorved kontrollen ikke kunne testes yderligere.</p> <p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

KONTROLMÅL E:

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

CompuSoft A/S' kontroller	Revisors test af kontroller	Resultat af test
<p>E.1 Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne.</p> <p>Vi har inspiceret, at procedurerne er opdateret.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>E.2 Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.</p>	<p>Vi har inspiceret, at der er dokumentation for at, at databehandlingen alene foretages på de lokaliteter der fremgår af databehandleraftalen.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

KONTROLMÅL F:

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

CompuSoft A/S' kontroller	Revisors test af kontroller	Resultat af test
<p>F.1 Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til databehandlerens anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>F.2 Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.</p>	<p>Vi har inspiceret, at den anvendte underdatabehandler fremgår af databehandleraftalerne.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>F.3 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.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer for underretning af den dataansvarlige ved ændringer i anvendelse af underdatabehandlere.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>F.4 Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.</p>	<p>Vi har inspiceret, at der er indgået databehandleraftaler med den godkendte underdatabehandler.</p> <p>Vi har inspiceret, at denne databehandleraftaler indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

<p>F.5 Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af:</p> <ul style="list-style-type: none"> • Navn • CVR.nr. • Lokation • Beskrivelse af behandlingen 	<p>Vi har inspiceret, at databehandler har en oversigt over godkendte underdatabehandlere der, som minimum, indeholder de krævede oplysninger om de enkelte underdatabehandlere.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>F.6 Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.</p>	<p>Vi har inspiceret, at der risikovurderingen indeholder forhold ved underdatabehandlere.</p> <p>Vi har inspiceret, at der er modtaget dokumentation for forholdene ved leverandører, herunder certificeringer og revisionserklæringer.</p> <p>Vi har forespurgt, hvorvidt der foretages opfølgning og gennemgang af modtaget materiale.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

KONTROLMÅL G:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.

CompuSoft A/S' kontroller	Revisors test af kontroller	Resultat af test
<p>G.1 Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har 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.</p> <p>Vi har inspiceret, at procedurerne er opdateret.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>G.2 Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.</p>	<p>Vi har inspiceret, at indgåede databehandleraftaler indeholder krav om instruks ved overførsel til tredjelande eller internationale organisationer.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>G.3 Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.</p>	<p>Vi har forespurgt, om CompuSoft A/S har vurderet hvorvidt der eksisterer et gyldigt overførselsgrundlag ved mulige overførsler af personoplysninger til tredjelande.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

KONTROLMÅL H:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.

CompuSoft A/S' kontroller	Revisors test af kontroller	Resultat af test
<p>H.1 Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har inspiceret, at der foreligger formaliserede krav til databehandlers bistand i relation til de registreredes rettigheder.</p> <p>Vi har inspiceret, at procedurerne er opdateret.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>H.2 Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer for bistand til den dataansvarlige herunder:</p> <ul style="list-style-type: none"> • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsninger til behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. <p>Vi har inspiceret, at platformen muliggør at dataansvarlig selv kan opfylde størstedelen af forpligtelserne over for den registrerede.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

KONTROLMÅL I:

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

CompuSoft A/S' kontroller	Revisors test af kontroller	Resultat af test
<p>I.1 Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har inspiceret, at der foreligger formaliserede procedurer, der indeholder krav om underretning af de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Vi har inspiceret, at proceduren er opdateret.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>I.2 Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden:</p> <ul style="list-style-type: none"> • Awareness hos medarbejdere • Overvågning af netværkstrafik • Opfølgning på hændelser i systemer og databaser 	<p>Vi har inspiceret, at medarbejdere er løbende orienteret om procedurer ved mistanke om databrud.</p> <p>Vi har inspiceret dokumentation for, at netværkstrafik monitoreres og der sker opfølgning ved anomaliteter.</p> <p>Vi har forespurgt om der sker opfølgning på hændelser i systemer og databaser.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>I.3 Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødigt forsinkelse, efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.</p>	<p>Vi har inspiceret, at der foreligger en ajourført oversigt over brud og mulige brud persondatasikkerheden, samt nærved-hændelser.</p> <p>Vi har inspiceret, at der ikke fremgår hændelser der har krævet orientering af dataansvarlige.</p>	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>
<p>I.4 Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet:</p> <ul style="list-style-type: none"> • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. 	<p>Vi har inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder procedurer for:</p> <ul style="list-style-type: none"> • 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. 	<p>Vi har ikke ved vores test konstateret væsentlige afvigelser.</p>

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.”

Thomas Traberg-Larsen

Direktør

Serienummer: ee7c1f22-5d6e-4c50-9aa4-77798af01e8f

IP: 212.98.xxx.xxx

2024-04-30 06:49:29 UTC



Jens Theodor Saugbjerg

BEIERHOLM, STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR:

32895468

IT-auditor

Serienummer: 9b5b6963-b085-4bcb-a035-209d426956e1

IP: 212.98.xxx.xxx

2024-04-30 06:50:06 UTC



Kim Holm Larsen

BEIERHOLM, STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR:

32895468

Statsautoriseret Revisor

Serienummer: bff7239f-6800-4339-865f-dbc13a357020

IP: 212.98.xxx.xxx

2024-04-30 07:44:50 UTC



Penneo dokumentnøgle: DAPTW-C7ADS-D8V1L-N5EDA-LE821-HMLTY

Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstempelt med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

Sådan kan du sikre, at dokumentet er originalt

Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet

i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service <penneo@penneo.com>**. Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske signeringsbeviser indlejret i dokumentet ved at anvende Penneos validator på følgende websted: **https://penneo.com/validator**