

RelateIT A/S

Uafhængig revisors ISAE 3000-erklæring pr. 15. maj 2023 med sikkerhed om informationssikkerhed og foranstaltninger rettet mod databeskyttelse og behandling af personoplysninger i forbindelse med leverance af RelateIT's ydelser

Pr. 15. maj 2023

Indholdsfortegnelse

1. Uafhængig revisors erklæring	1
2. Ledelsens udtalelse	3
3. Systembeskrivelse	5
4. RelateIT's kontrolmål, kontroller, test og resultat heraf.....	9

1. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring pr. 15. maj 2023 med sikkerhed om informationssikkerhed og foranstaltninger rettet mod databeskyttelse og behandling af personoplysninger i forbindelse med leverance af RelateIT's ydelser

Til: RelateIT og deres kunder, som anvender RelateIT til at håndtere persondata i Microsofts applikationer

Omfang

Vi har fået til opgave at afgive erklæring om RelateIT A/S' (herefter 'RelateIT') beskrivelse i afsnit 3 af RelateIT's services i henhold til databehandleraftalen med dataansvarlig pr. 15. maj 2023 (beskrivelsen) samt om udformningen og implementeringen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

RelateIT anvender serviceunderleverandøren RelateIT DMCC. RelateIT's systembeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos serviceunderleverandøren. Denne erklæring er udarbejdet efter partielmetoden og omfatter således ikke kontroller hos serviceunderleverandøren.

Enkelte af de kontrolmål, der er anført i RelateIT's beskrivelse af sit system, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos RelateIT. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementerende kontroller.

Vores konklusion udtrykkes med høj grad af sikkerhed.

RelateIT's ansvar

RelateIT er ansvarlig for udarbejdelsen af beskrivelsen og den tilhørende udtalelse i afsnit 2, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret, for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene og for at 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 IESBA's Etiske regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

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

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om RelateIT'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, *Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger*, og yderligere krav ifølge dansk revisorlovgivning, med henblik på at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og implementeret.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og implementeringen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i RelateIT's beskrivelse af sin ydelse samt for kontrollerens udformning og implementering. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet. Vores handlinger har omfattet test af udformning og implementering af de kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået.

En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som RelateIT har specificeret og beskrevet i afsnit 2.

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

Begrænsninger i kontroller hos en dataansvarlig

RelateIT'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 RelateIT's services, 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 fremskrivning af enhver vurdering af implementering 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 RelateIT's services, således som denne var udformet og implementeret pr. 15. maj 2023, i alle væsentlige henseender er retvisende
- (b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet og implementeret pr. 15. maj 2023.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller, som fremgår af afsnit 4, er udelukkende tiltænkt de dataansvarlige, der har anvendt RelateIT's services, 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.

København, den 9. august 2023

Deloitte

Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56

Thomas Kühn
partner, statsautoriseret revisor

2. Ledelsens udtalelse

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

RelateIT bekræfter, at:

- a) Den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af RelateIT's service, der har behandlet personoplysninger for dataansvarlige, der er omfattet af databeskyttelsesforordningen, pr. 15. maj 2023. De kriterier, der er anvendt for at give denne udtalelse, var, at den medfølgende beskrivelse:
- (i) Redegør for, hvordan systemet var udformet og implementeret, herunder redegør for:
- De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
 - De processer i både it- og manuelle systemer, der er anvendt til at igangsætte og registrere behandling af personoplysninger og om nødvendigt korrigere eller slette personoplysninger og begrænse behandling af personoplysninger
 - De processer, der er anvendt til 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 sikringsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandlingen udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet
 - Kontroller, som vi med henvisning til systemets afgrænsning har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen
 - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger.
- (ii) Indeholder relevante oplysninger om ændringer ved RelateIT's service til behandling af personoplysninger foretaget pr. 15. maj 2023.
- (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne system til behandling af personoplysninger under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved RelateIT's virke, som den enkelte dataansvarlige måtte anse for vigtigt efter dennes særlige forhold.
- b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. 15. maj 2023. De kriterier, der er anvendt for at give denne udtalelse, var, at:
- (i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret.
- (ii) De identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål.

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

Odense, den 9. august 2023

På vegne af RelateIT A/S

Simon Berthelsen
Managing Director and Partner

Carsten Andersen
Managing Partner

3. Systembeskrivelse

3.1 Indledning

Denne beskrivelse er udfærdiget med henblik på at levere information til brug for RelateIT's kunder og revisorer omkring efterlevelse af GDPR-forordningen i de leverancer, som RelateIT leverer til kunder, og som RelateIT i sin egenskab af underleverandør har helt eller delvist ansvar for.

Erklæringen er organiseret med udgangspunkt i ISAE 3000-rammeverket og opsat efter de kontroller, som indgår i rammeverket fra FSR.

Nærværende sektion indeholder beskrivelse af de artikler i GDPR-loven, som er relevante for RelateIT's leverancer, og som RelateIT har ansvar for at efterleve. RelateIT er underleverandør og ikke dataansvarlig i leverancer og efterlever de krav, som kunder som dataansvarlige har fremsat igennem aftalegrundlag og databehandleraftaler.

RelateIT er en af landets største NAV-/Business Central-partnere, som leverer ambitiøse ERP-konsulent-ydelser til virksomheder med både nationale og internationale udviklingsbehov. Vi leverer også løsninger til din IT-infrastruktur, som sikrer jeres fremtidige drift og indfrier kravene til moderne IT. RelateIT er en rådgivende virksomhed, der har til formål at levere IT-ydelser til kunder baseret på Microsofts løsninger. RelateIT er en af Danmarks største Microsoft Dynamics 365 Business Central- /NAV-partnere, som leverer ERP-løsninger til virksomheder med både nationale og internationale udviklingsbehov. Derudover leverer vi også løsninger indenfor Business Intelligence, Power Automate, e-commerce, web, IT-infrastruktur og IT-sikkerhed, så kunderne får en integreret løsning, der sikrer fremtidig drift og indfrier kravene til moderne IT.

3.2 Beskrivelse af RelateIT's ydelser

Om os og vores IT-kerne-ydelser

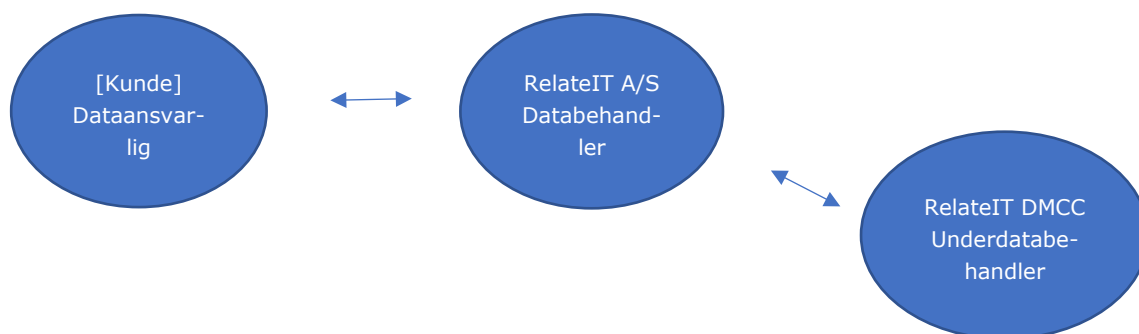
Vores kompetencer spænder bredt. De væsentligste ydelser er:

- Konsulent-ydelser og udvikling på Microsoft Business Central/ NAV & LS Central
- Salg af ISV-løsninger
- Digitalisering og automatisering af forretningsprocesser
- Business Intelligence
- Microsoft Power Platform & Power Automate
- Udvikling af skræddersyede webløsninger
- IT Service Management.

For at levere ovenstående ydelser og udføre IT-arbejdet eller yde support har de medarbejdere, der arbejder på den enkelte kunde, adgang til kundens platform.

3.3 Underdatabehandlere

Illustration af sammenhængen mellem dataansvarlig, databehandler og tredjepartsdatabehandler:



RelateIT anvender underdatabehandler RelateIT DMCC, som er registreret i De Forenede Arabiske Emirater (Dubai).

RelateIT DMCC anvendes i de tilfælde, hvor der kan være behov for at assistere RelateIT A/S med udvikling og opsætning i samme omfang. Der er indgået en underdatabehandleraftale med RelateIT DMCC og dermed er det sikret, at RelateIT DMCC er underlagt samme politikker og procedurer som RelateIT A/S. RelateIT DMCC's medarbejdere følger RelateIT's procedurer, kontroller og politikker mv.

3.4 Karakteren af behandlingen

RelateIT leverer services relateret primært til rådgivning og assistance til kunden, hvor vi udfører opsætning, migrering, test, udvikling mv. Typerne af aktiviteter vil typisk vedrøre følgende:

- Udførelse af tests af udviklede software- eller hardwareløsninger for Kunden
- Analyser og fejlfinding i Kundens IT-systemer
- Migrering af data mellem Kundens IT-systemer.

RelateIT kommer i forbindelse med udførelse af ydelser hos kunderne i berøring med kundernes persondata. Personoplysningerne bliver altid behandlet på kundens platform. RelateIT's databehandling kan derfor kun blive udført på kundens platform.

RelateIT's behandling af personoplysninger på vegne af den dataansvarlige er yderligere dokumenteret via den underskrevne databehandleraftale.

3.5 Kontrolforanstaltninger

RelateIT's behandling af personoplysninger i forbindelse med udførelse af ydelser hos kunderne sker kun på kundernes platform. Derfor foretages der ikke behandling af personoplysninger i RelateIT's systemer og databaser.

Endvidere foretager RelateIT ikke overførsel af personoplysninger fra kundernes platform i forbindelse med RelateIT's ydelser. Derfor er det kundernes ansvar at etablere passende sikkerhedsforanstaltninger i relation til behandling af personoplysninger, som fx kan være backup, kryptering, logning mv.

RelateIT har implementeret kontrolforanstaltninger, som sikrer, at RelateIT's behandling af kundernes persondata sker på baggrund af de risici, som er identificeret.

Nedenfor fremgår kortfattede beskrivelser af RelateIT's kontroller og foranstaltninger indenfor de områder, som er omfattet af nærværende erklæring.

- Databehandleraftaler og instruks (kontrolmål A)
- Tekniske sikringsforanstaltninger (kontrolmål B)
- Organisatoriske foranstaltninger (kontrolmål C)
- Anvendelse af underdatabehandlere (kontrolmål F)
- Overførsel til tredjeland (kontrolmål G)
- Håndtering af sikkerhedsbrud (kontrolmål I).

3.5.1 Generelle procedurer for behandling af personoplysninger (kontrolmål A)

Formål

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

Anvendte procedurer og kontroller

RelateIT har udarbejdet procedurer, der sikrer, at der kun behandles persondata efter instruks fra dataansvarlige. Der føres løbende kontrol med, at persondata behandles efter instruks, og der er etableret procedurer for underretning af den dataansvarlige, hvis behandlingen er i strid med lovgivningen. Alle medarbejdere hos RelateIT orienteres løbende om dette gennem undervisning og awareness-træning.

3.5.2 Tekniske sikringsforanstaltninger (kontrolmål B)

Formål

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

Anvendte procedurer og kontroller

Som nævnt tidligere foretager RelateIT behandling af personoplysninger kun på kundernes platform.

Derfor er det kundernes ansvar at etablere passende sikkerhedsforanstaltninger i relation til behandling af personoplysninger, som fx kan være backup, kryptering, logning mv.

Nedenfor er en beskrivelse af de sikkerhedsforanstaltninger, som er etableret hos RelateIT.

RelateIT har udarbejdet en risikovurdering, som omfatter en beskrivelse af de tekniske foranstaltninger, der skal sikre en passende sikkerhed hos RelateIT, som er i overensstemmelse med risikovurderingen.

Adgang til personoplysninger er begrænset til interne medarbejdere i RelateIT, som har et arbejdsbetinget behov for adgang. Organisationens systemer har logisk adgangskontrol i form af brugernavn og adgangskode eller anden autorisation. Der er procedurer for tildeling af autorisationer til IT-systemer ved en medarbejders ansættelse. Adgangstildelingen skal godkendes efter gældende procedure, og alle adgange gennemgås af relevant personale.

RelateIT tildeler enkelte eller grupper af brugere autorisation til at tilgå, ændre og slette behandlede personoplysninger. Der er procedurer for tilbagekaldelse af tilladelser, når en medarbejder stopper i organisationen eller skifter afdeling.

Der foretages regelmæssig gennemgang og kontrol af brugerautorisationer til specifikke systemer.

E-mails bliver krypteret centralt hos RelateIT. Alle e-mails er TLS-krypteret i transit.

3.5.3 Organisatoriske foranstaltninger (kontrolmål C)

Formål

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

Anvendte procedurer og kontroller

RelateIT har implementeret passende organisatoriske foranstaltninger. Foranstaltningerne omfatter fastlæggelse af politikker for IT-sikkerhed, som offentliggøres og kommunikeres til medarbejdere og relevante kontrahenter. Derudover er der implementeret procedurer, der sikrer fortrolighed samt løbende uddannelse og awareness-træning.

3.5.4 Anvendelse af underdatabehandlere (kontrolmål F)

Formål

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

Anvendte procedurer og kontroller

RelateIT anvender underdatabehandler RelateIT DMCC, som er registreret i De Forenede Arabiske Emirater (Dubai).

RelateIT DMCC anvendes i de tilfælde, hvor der kan være behov for at assistere RelateIT A/S med udvikling og opsætning i samme omfang. Der er indgået en underdatabehandleraftale med RelateIT DMCC, og det er dermed sikret, at RelateIT DMCC er underlagt samme politikker og procedurer som RelateIT A/S.

Databehandler overfører ikke personoplysninger til tredjelande.

3.5.5 Overførsel til tredjeland (kontrolmål G)

Formål:

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.

Anvendte procedurer og kontroller

Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.

Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige. Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.

3.5.6 Sikkerhedsbrud (kontrolmål I)

Formål

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

Anvendte procedurer og kontroller

RelateIT har procedurer og kontroller til at identificere og håndtere brud på persondatasikkerheden, herunder underretning af den Dataansvarlige og eventuel assistance til den Dataansvarlige ved den Dataansvarliges anmeldelse af brud på persondatasikkerheden til den relevante tilsynsmyndighed.

RelateIT har en dokumenteret procesbeskrivelse for brud på persondatasikkerheden. Der er etableret processer for, at RelateIT's medarbejdere kan dokumentere og rapportere på brud på datasikkerheden eller risici herfor.

3.6 Komplementerende kontroller hos de dataansvarlige

RelateIT leverer ydelser på baggrund af databehandleraftale, og derfor er der en række kontroller, som den dataansvarlige har til ansvar for efterleves, herunder;

- At sikre, at personoplysninger er ajourførte
- At databehandleraftalen er lovlige i forhold til gældende persondataretlig regulering
- At databehandleraftalen er retvisende i forhold til leverancens omfang
- At der er udarbejdet risikovurdering af behandling af personoplysninger, herunder en konsekvensvurdering af behandling af persondata
- At der er etableret passende kontroller til sikring af adgangs- og rettighedsstyring for egne medarbejdere og brugere
- At der er etableret relevante, passende sikkerhedsforanstaltninger i relation til behandling af personoplysninger, herunder overvågning, netværkssegmentering, installering af antivirus mv.
- Bistand til den registrerede, herunder bistand, der udføres via kundernes egne værktøjer.

4 RelateIT's kontrolmål, kontroller, test og resultat heraf

4.1 Introduktion

Denne rapport er udformet med henblik på at informere kunder om RelateIT's services og kontroller, som kan påvirke behandlingen af personoplysninger, og samtidig informere de dataansvarlige, for hvem RelateIT behandler personoplysninger, om implementering af de kontroller, der blev efterprøvet. Afsnittet, når det kombineres med en forståelse og vurdering af kontrollerne hos de dataansvarlige, har til hensigt at hjælpe de dataansvarlige til at vurdere risici forbundet med den outsourcete behandling af personoplysninger, som muligvis påvirkes af kontrollerne hos RelateIT.

Vores test af RelateIT's kontroller er begrænset til de kontrolmål og relaterede kontroller, som er nævnt i nedenstående kontrolmatrix i denne del af rapporten, og er ikke udvidet til at omfatte alle de kontroller, som er beskrevet i systembeskrivelsen, eller kontroller, som forventes at være implementeret hos de dataansvarlige for at opfylde kontrolmålene.

Det er den dataansvarliges ansvar at evaluere denne information i forhold til de kontroller, som eksisterer hos den dataansvarlige. Hvis bestemte komplementerende kontroller ikke er til stede hos den dataansvarlige, kan RelateIT's kontroller muligvis ikke kompensere for sådanne svagheder.

4.2 Test af kontroller

De udførte test i forbindelse med fastlæggelse af kontrollers funktionalitet består af en eller flere af følgende metoder:

Metode	Beskrivelse
Forespørgsel	Forespørgsel hos udvalgt personale hos RelateIT
Observation	Observation af kontrollens udførelse
Inspektion	Inspektion af dokumenter og rapporter, som angiver udførelse af kontroller. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er udformet og implementeret pr. 15. maj 2023.
Genudførelse af kontrollen	Gentagelse af den relevante kontrol med henblik på at verificere, at kontrollen fungerer som forudsat.

4.3 Kontrolmål, kontroller og resultater af test

Vores test af kontrollernes udformning og implementering inkluderer de test, som vi betragter som nødvendige for at vurdere, om de udførte kontroller og overholdelsen heraf er tilstrækkelige til at give høj, men ikke absolut sikkerhed for, at de specificerede kontrolmål blev opnået pr. 15. maj 2023.

4.4 Kontrolmål, kontroller og resultater af test

I nedenstående skema er de testede kontrolmål og kontroller anført, ligesom vi har beskrevet, hvilke revisionshandling der er udført og resultatet af disse handlinger. I det omfang vi har konstateret væsentlige kontrolsvagheder, har vi anført dette.

4.5 Kontrolmål, kontrolaktivitet, test og resultat heraf

Kontrolmål A			
Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
A.1	<p>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>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.</p> <p>Deloitte har inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen.</p> <p>Deloitte har inspiceret, at procedurer er opdateret.</p>	Ingen afvigelser konstateret.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	<p>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har inspiceret relevant dokumentation, hvoraf det fremgår, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.</p> <p>Deloitte har inspiceret én stikprøve på en databehandleraftale og observeret, at den omfatter bestemmelser om, at behandling af personoplysninger foregår i overensstemmelse med instruks.</p>	Ingen afvigelser konstateret.
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	<p>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning.</p> <p>Deloitte har på forespørgsel fået oplyst, at der på revisionstidspunktet ikke har været tilfælde af den karakterer, hvor behandling af personoplysninger blev vurderet i strid med databeskyttelsesforordningen, og den dataansvarlige skulle underrettes.</p>	Ingen afvigelser konstateret.

Kontrolmål B			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
B.1	<p>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>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger.</p> <p>Deloitte har inspiceret, at procedurer er opdateret.</p> <p>Deloitte har inspiceret ved én stikprøve på en databehandleraftale, at der er etableret de aftalte sikringsforanstaltninger.</p>	Ingen afvigelser konstateret.
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>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed.</p> <p>Deloitte har inspiceret risikovurderingen og observeret, at den bl.a. omfatter en beskrivelse af behandling af personoplysninger.</p> <p>Deloitte har inspiceret, at der er i risikovurderingen, er beskrevet de tekniske foranstaltninger, som skal sikre en passende sikkerhed i overensstemmelse med risikovurderingen.</p> <p>Deloitte har inspiceret ved én stikprøve på en databehandleraftale, at den omfatter krav til sikringsforanstaltninger hos databehandleren.</p>	<p>Det er konstateret, at risikovurderingen er fra den 10.06.2022.</p> <p>Ingen yderligere afvigelser konstateret.</p>
B.6	Adgang til personoplysninger er isoleret til brugere med et arbejdsbetinget behov herfor.	<p>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger.</p>	Ingen afvigelser konstateret.

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

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
		<p>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov.</p> <p>Deloitte har inspiceret relevant dokumentation, hvoraf det fremgår, at de aftalte tekniske foranstaltninger understøttes, og brugernes adgangsbegrænsninger opretholdes.</p> <p>Deloitte har ved én stikprøve på en medarbejder inspiceret relevant dokumentation og observeret, at adgangsautorisation til systemer og data er godkendt og begrænset til medarbejderens arbejdsbetingede behov.</p>	
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og pr. e-mail.	<p>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme.</p> <p>Deloitte har inspiceret, at RelateIT anvender kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller pr. e-mail.</p> <p>Deloitte har på forespørgsel fået oplyst, at al behandling af personoplysninger foretages på kundernes platform, og dermed er det de dataansvarlige, som har ansvaret på området.</p> <p>Deloitte har fået oplyst, at der ikke foretages transmission af kundernes fortrolige og følsomme personoplysninger ud af kundernes platform i forbindelse med RelateIT's levering af ydelser hos kunderne.</p>	Ingen afvigelser konstateret.

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

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugerens adgange revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	<p>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger.</p> <p>Deloitte har ved én stikprøve på en medarbejder inspiceret relevant dokumentation og observeret, at adgang til systemer og databaser er godkendt og begrænset til et arbejdsbetinget behov.</p> <p>Deloitte har ved én stikprøve på en fratrådt medarbejder inspiceret, at rettigheder er rettidigt deaktiveret.</p> <p>Deloitte har inspiceret, at der foreligger dokumentation for regelmæssig – mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.</p>	Ingen afvigelser konstateret.

Kontrolmål C

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
C.1	<p>Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere.</p>	<p>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt.</p> <p>Deloitte har inspiceret, at der er udarbejdet følgende relevante politikker relateret til informationssikkerheden:</p> <ul style="list-style-type: none"> • Account Management & Access Control • Awareness policy • Password policy • Policy for maintenance, repair, disposal and re-use of hardware • Shadow IT policy. <p>Deloitte har inspiceret dokumentation for, at informationssikkerhedspolitikkerne er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.</p>	<p>Ingen afvigelser konstateret.</p>
C.2	<p>Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i strid med indgåede databehandleraftaler.</p>	<p>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler.</p> <p>Deloitte har inspiceret ved én stikprøve på en databehandleraftale, at kravene i aftalen er dækket af informationssikkerhedspolitikens krav til sikringsforanstaltninger og behandlingssikkerheden.</p>	<p>Ingen afvigelser konstateret.</p>
C.3	<p>Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang:</p> <ul style="list-style-type: none"> • Referencer fra tidligere ansættelser 	<p>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.</p>	<p>Ingen afvigelser konstateret.</p>

Kontrolmål C

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
	<ul style="list-style-type: none"> • Straffeattest. 	Deloitte har forespurgt ved én stikprøve på en nyansat medarbejder om processen for efterprøvning i forbindelse med ansættelse og har fået oplyst, at der blev indhentet referencer fra tidligere ansættelser og straffeattest.	
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til relevante politikker og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	<p>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har ved én stikprøve på en nyansat medarbejder på revisionstidspunktet inspiceret, at den pågældende medarbejder har underskrevet en fortrolighedsaftale.</p> <p>Deloitte har inspiceret ved én stikprøve på en nyansat medarbejder, at den pågældende medarbejder er blevet introduceret til:</p> <ul style="list-style-type: none"> • Medarbejderhåndbogen • Intro til Team Infrastruktur. 	Ingen afvigelser konstateret.
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>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har inspiceret procedurer, der sikrer, at fratrådte medarbejders rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages</p> <p>Deloitte har ved én stikprøve på en fratrådt medarbejder inspiceret, at rettigheder er inaktiveret, og at aktiver er inddraget.</p>	Ingen afvigelser konstateret.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, og at medarbejderen er underlagt en generel tavshedspligt i relation til den behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	<p>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt.</p>	Ingen afvigelser konstateret.

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
		Deloitte har ved én stikprøve på en fratrådt medarbejder inspiceret relevant dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt.	
C.7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til generel it-sikkerhed.	<p>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har inspiceret procedure for awareness-træning.</p> <p>Deloitte har inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed.</p> <p>Deloitte har forespurgt, om RelateIT har gennemført awareness-træning af medarbejderne om generel IT-sikkerhed og behandlingssikkerhed i relation til personoplysninger.</p>	Ingen afvigelser konstateret.

Kontrolmål F

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Deloitte har inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret ved én stikprøve på en underdatabehandler, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne og er godkendt af den dataansvarlige.	Ingen afvigelser konstateret.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har ved én stikprøve på en databehandleraftale inspiceret, at den omfatter krav om underretning af den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Deloitte har på forespørgsel fået oplyst, at der på revisionstidspunktet ikke har været ændringer ved anvendelse af underdatabehandlerne, og derfor blev der ikke foretaget yderligere.	Ingen afvigelser konstateret.
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.	Ingen afvigelser konstateret.

Kontrolmål F

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
		<p>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har inspiceret ved én stikprøve på en underdatabehandleraftale og observeret, at den indeholder samme krav og forpligtelser som dem, der er anført i databehandleraftalen mellem de dataansvarlige og databehandleren.</p>	
F.5	<p>Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af:</p> <ul style="list-style-type: none">• Navn• CVR-nr.• Adresse	<p>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har forespurgt, om databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere.</p> <p>Deloitte har inspiceret én databehandleraftale og observeret, at der indgår en oversigt over underdatabehandler, der som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.</p>	Ingen afvigelser konstateret.
F.6	<p>Databehandleren foretager opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne.</p>	<p>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har forespurgt til procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne.</p> <p>Deloitte har inspiceret relevant dokumentation, hvoraf det fremgår, at underdatabehandleren bekræfter opfyldelsen af krav, jf. underdatabehandleraftalen.</p>	Ingen afvigelser konstateret.

Kontrolmål G

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.	<p>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har forespurgt, om 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>Deloitte har inspiceret dokumentet "Databehandlerprocedure" og observeret, at der er beskrevet 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>Deloitte har inspiceret ved én stikprøve på en underdatabehandleraftale og observeret, at den indeholder krav vedrørende overførsel af personoplysninger til tredjelande eller internationale organisationer.</p>	Ingen afvigelser konstateret.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	<p>Deloitte har forespurgt udvalgt personale om kontrollen.</p> <p>Deloitte har inspiceret dokumentet "Databehandlerprocedure" og observeret, at der er beskrevet krav om instruks fra den dataansvarlige ved eventuel overførsel af personoplysninger til tredjelande eller internationale organisationer.</p> <p>Deloitte har inspiceret ved én stikprøve på en underdatabehandleraftale og observeret, at den omfatter instruks vedrørende overførsel af personoplysninger til tredjelande.</p>	Ingen afvigelser konstateret.
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>Deloitte har forespurgt udvalgt personale om kontrollen.</p>	Ingen afvigelser konstateret.

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.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
		<p>Deloitte har inspiceret dokumentet "Databehandlerprocedure" og observeret, at der er beskrevet krav om instruks vedrørende et gyldigt overførselsgrundlag fra den dataansvarlige ved overførsel af personoplysninger til tredjelande eller internationale organisationer.</p> <p>Deloitte har inspiceret ved én stikprøve på en underdatabehandleraftale og observeret, at den omfatter instruks for lovlige overførselsgrundlag i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer.</p>	

Kontrolmål I			
Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandlersaftale.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at proceduren er opdateret.	Ingen afvigelser konstateret.
I.2	Databehandleren har etableret følgende kontroller for identificering af eventuelle brud på persondatasikkerheden: <ul style="list-style-type: none"> • Der er udarbejdet procedure for håndtering af informationssikkerhedsbrud og informationssikkerhedshændelser. • Alle medarbejdere introduceres til håndtering af informationssikkerhedsbrud og informationssikkerhedshændelser. 	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret proceduren for identificering af eventuelle brud på persondatasikkerheden og observeret, at der er beskrevet krav om, at alle medarbejdere er ansvarlige for og forpligtede til at indberette sikkerhedshændelser og sårbarheder. Deloitte har på forespørgsel fået oplyst, at alle medarbejdere i forbindelse med deres ansættelse har været igennem introduktion og bekræftet at have læst bestemmelserne relateret til sikkerhedshændelser. Deloitte har inspiceret ved én stikprøve på en nyansat medarbejder, at den pågældende medarbejder er blevet introduceret til: <ul style="list-style-type: none"> • Medarbejderhåndbogen • Intro til Team Infrastruktur. 	Ingen afvigelser konstateret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødigt forsinkelse og senest 72 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Deloitte har forespurgt udvalgt personale om kontrollen. Deloitte har inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Deloitte har forespurgt, om der har været registeret brud på persondatasikkerheden, og har fået oplyst, at der på revisionstidspunktet ikke har været registreret brud på persondatasikkerheden.	Ingen afvigelser konstateret.

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

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
I.4	Databehandleren har procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet.	<p>Deloitte har inspiceret 'Databehandlerprocedure' og observeret, at der fremgår bestemmelser relateret til håndtering af sikkerhedsbrud, som skal håndteres i overensstemmelse med indgåede databehandleraftaler og eventuel assistance til den dataansvarlige ved anmeldelse af brud til Datatilsynet.</p> <p>Deloitte har på forespørgsel fået oplyst, at der på revisionstidspunktet ikke har været anmodninger om bistand fra de dataansvarlige.</p>	Ingen afvigelser konstateret.

PENNEO

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

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

Carsten Andersen

Intern underskriver

På vegne af: RelateIT

Serienummer: 48beff95-a05a-4a66-b244-8d287171b676

IP: 193.88.xxx.xxx

2023-08-09 16:14:48 UTC



Simon Eglin Berthelsen

Intern underskriver

På vegne af: RelateIT

Serienummer: 68265612-d69a-4f42-8fd5-2f8979c41897

IP: 80.208.xxx.xxx

2023-08-09 18:35:01 UTC



Thomas Kühn

Ekstern underskriver

På vegne af: Deloitte

Serienummer: d1fc228f-48ef-4abe-abad-efe9492b4894

IP: 83.151.xxx.xxx

2023-08-10 05:58:46 UTC



Penneo dokumentnøgle: VCUH1-003JG-XFTX(-TUJZ87-5J3OD-SMAEU

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 tidsstemplet 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 i indlejret i dokumentet ved at anvende Penneos validator på følgende websted: <https://penneo.com/validator>