Dansk Revision Århus
godkendt revisionsaktieselskab
Tomsagervej 2
DK-8230 Åbyhøj
aarhus@danskrevision.dk
www.danskrevision.dk
Telefon: +45 89 36 12 12
Telefax: +45 89 36 12 00
CVR: DK 26 71 76 71
Bank: 6181 0007769555

Berú A/S

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med Berú A/S´ kunder.

Indholdsfortegnelse

1. Ledelsens udtalelse 3
2. Uafhængig revisors erklæring 5
3. Systembeskrivelse 7
4. Kontrolmål, kontrolaktivitet, test og resultat heraf 14

1. Ledelsens udtalelse

Berú 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 Berú A/S' ydelser, 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. Berú A/S bekræfter, at:

a) Den medfølgende beskrivelse, giver en retvisende beskrivelse af, hvordan Berú A/S har behandlet personoplysninger på vegne af dataansvarlige i perioden fra den 1. februar 2023 til 31. januar 2024 Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan Berú A/S' processer og kontroller relateret til databeskyttelse var udformet og implementeret, herunder redegør for:

   - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
   - De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger
   - De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige
   - De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt
   - De processer, der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne
   - De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registrerede
   - De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet
   - Kontroller, som vi med henvisning til Berú 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
   - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og

overvågningskontroller, som har været relevante for behandlingen af personoplysninger

(ii) Indeholder relevante oplysninger om ændringer ved databehandlerens ydelser til behandling af personoplysninger foretaget fra den 1. februar 2023 til 31. januar 2024.

(iii) 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.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra den 1. februar 2023 til 31. januar 2024. Kriterierne anvendt for at give denne udtalelse var, at:

(i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret

(ii) De identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål, og

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra den 1. februar 2023 til 31. januar 2024

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

København S, 17. april 2024

Rasmus Ørgaard Rudolf

Adm. direktør

Berú A/S

Njalsgade 21 E st,

2300 København S

2. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med Berú A/S´ kunder relateret til ydelsen.

Til: Berú A/S og Berú A/S´ kunder relateret til ydelsen

Omfang

Vi har fået som opgave at afgive erklæring om Berú A/S' beskrivelse af ydelser i relation til behandling af personoplysninger på vegne af dataansvarlige i henhold til databehandleraftale med Berú A/S´ kunder i hele perioden fra den 1. februar 2023 til 31. januar 2024 om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Berú A/S anvender underleverandøren og underdatabehandleren Hetzner. Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos Berú A/S' underleverandører og underdatabehandlere.

Berú A/S' ansvar

Berú A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 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.

Revisors uafhængighed og kvalitetsstyring

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

Dansk Revision er underlagt international standard om kvalitetsstyring, ISQC 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 Berú A/S' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

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

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af Berú A/S' ydelser samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i afsnit 3.

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

Berú 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 Berú A/S' ydelser, 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 behandling af personoplysninger, således som denne var udformet og implementeret i perioden fra den 1. februar 2023 til 31. januar 2024 i alle væsentlige henseender er retvisende, og

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i perioden fra den 1. februar 2023 til 31. januar 2024, og

(c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i perioden fra den 1. februar 2023 til 31. januar 2024

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt dataansvarlige, der har anvendt Berú A/S' GoBasic løsning, 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.

Åbyhøj, 17. april 2024

Dansk Revision Århus
godkendt revisionsaktieselskab, CVR-nr. 26717671

Claus Guldborg Nyvold
registreret revisor
mne29387

3. Beskrivelse af behandling

Formålet med denne beskrivelse at give specifikke oplysninger om spørgsmål vedrørende sikkerheden ved behandling, tekniske og organisatoriske foranstaltninger, ansvar mellem dataansvarlige (vores kunder) og processoren (Berú ApS), og hvordan de tilbudte tjenester kan hjælpe med at understøtte de registreredes rettigheder.

Vores kontrolmål, herunder regler og procedurer samt gennemførte kontroller

Berú ApS udvikler websites til private og offentlige kunder. Herunder udarbejdelse af design, opbygning og efter lancering, drift og support.

Principper vedrørende behandling af personoplysninger

Berú ApS har implementeret en informationssikkerhedspolitik der indeholder interne krav til it-sikkerheden, samt retningslinjer for os som databehandlere overfor vores dataansvarlige kunder.

Berú ApS anvender underdatabehandlere til hosting af servere, herunder og Hetzner, som er ISO 27001 certificeret.

Risikostyring i Berú ApS

Berú ApS har foretaget en risikovurdering på de behandlingsaktiviteter der udføres for kunderne, herunder en vurdering af de relevante trusler og sandsynlighed og konsekvens ved personoplysninger tab af fortrolighed, integritet og tilgængelighed.

Organisation og ansvar

Det er direktøren Rasmus Rudolf der har det overordnede ansvar for informationssikkerheden og behandlingen af personoplysninger i virksomheden.

Databehandleraftaler med kunder

Der indgås altid en databehandleraftale med den dataansvarlige før en behandling påbegyndes.

Databehandleraftalen indeholder som minimum:

- Typen af personoplysninger som behandles
- Varigheden af behandling
- Hvilken form for behandling der skal foretages og til hvilket formål
- Hvilke kategorier af registrerede de behandlede personoplysninger vedrører
- Den dataansvarliges rettigheder og forpligtelser
- At databehandleren kun må behandle personoplysningerne på baggrund af dokumenterede in-struktioner fra den dataansvarlige
- At personer hos databehandleren, der er autoriserede til at behandle oplysningerne, er underlagt fortrolighedsforpligtigelse
- At databehandleren etablerer passende sikkerhedsforanstaltninger
- At databehandleren overholder betingelser i forordningen for at bruge underdatabehandlere (arti-kel 28, stk. 2)
- At databehandleren bistår den dataansvarlige med at opfylde dennes forpligtelser over for den registrerede

- At databehandleren skal bistå den dataansvarlige med at sikre dennes overholdelse af forpligtigelserne i forordningens artikel 32-36 om bl.a. sikkerhedsforanstaltninger, anmeldelse ved sikkerhedsbrud, udarbejdelse af risikoanalyser, herunder eventuelt en DPIA og eventuel konsultation med databeskyttelsesmyndighederne
- At databehandleren på den dataansvarliges anmodning og efter den dataansvarliges valg sletter eller returnerer de behandlede personoplysninger ved behandlingens ophør
- At databehandleren udleverer alle nødvendige informationer med henblik på, at den dataansvar-lige kan dokumentere, at behandlingen hos databehandleren lever op til forpligtelserne, samt tillader og medvirker til kontrol og audits heraf. Herunder skal databehandleren være forpligtet til at informere den dataansvarlige, såfremt det er databehandlerens opfattelse at en instruks er ulovlig.

Det er Rasmus Rudolfs ansvar er der bliver indgået databehandleraftaler med kunder.

Behandling af oplysninger iht instruks

Vi sikrer os at vi udelukkende behandler personoplysninger iht. instruksen i de indgåede databehandleraftaler. Påstås der tvivl om instruksen kontaktes kunden før behandlingen påbegyndes.

Marketing og markedsføringsbrug

Vi benytter ikke personoplysninger vi behandler på vegne af en kunde til marketing eller markedsførings-brug, uden at vi har fået samtykke hertil fra de registrerede. Det må ikke være en betingelse for vores behandling at vores kunder skaffer et samtykke til markedsføring fra de registrerede.

Lovgivningsstridige instruks

Hvis vi vurderer at den instruks vi har fået fra kunden, er i strid med lovgivningen informerer vi kunden herom.

Kundeforpligtelser

Vi er villige til at deltage i audits fra vores kunder, herunder at levere en årlig revisorerklæring således at kunden kan demonstrere compliance hos os som databehandler.

De registreredes rettigheder

Som databehandler skal vi bidrage til at vores kunder kan imødekomme de registreredes rettigheder. Ved henvendelser fra vores kunder og hvor det er nødvendigt, assisterer vi kunden med sletning, berigtigelse, indsigt, udlevering af data etc.

Tilbagelevering, overførsel eller bortskaffelse af personoplysninger

Når et kundeforhold ender, skal vi enten foretage tilbagelevering, overførsel eller bortskaffelse af personoplysninger. Instruksen herom er defineret i databehandleraftalen med kunden.

Ved tilbagelevering og overførsel sørger vi for at dette foregår over en krypteret linje.

Ved bortskaffelse sørger vi for at personoplysninger uigenkaldeligt slettes ved overskrivning eller effektiv destruktion af hardware.

Transmission

Personoplysninger overføres på sikker vis. Alle følsomme eller fortrolige personoplysninger overføres over en krypteret forbindelse, minimum TLS 1.2.

Overførsel til usikre tredjelande

Vi overfører ikke til tredjelande. Vi informerer kunden såfremt vi ønsker at overføre personoplysninger vi behandler på deres vegne til usikre tredjelande, således at kunden har mulighed for at gøre indsigelse.

Oplysning om brug af underdatabehandlere

Via databehandleraftalen oplyser vi vores kunder om brug af underdatabehandlere.

Brug af underdatabehandlere

Vi skal have godkendelse til at benytte underdatabehandlere til at behandle personoplysninger på vegne af vores kunder. Når denne godkendelse af afgivet, indgår vi databehandleraftaler med underdatabehandlere. I instruksen til underdatabehandleren kræver vi som minimum det samme niveau af sikkerhed hos under-databehandleren som kunden kræver af os.

Kontrol med underdatabehandler

Der foretages en risikovurdering på underdatabehandlere med det formål at definere den korrekte metode at føre tilsyn på. Når vurderingen foretages, tages der stilling til hvilke typer af oplysninger som underdata-behandleren behandler for os, samt vores vurdering af deres tekniske og organisatoriske foranstaltninger.

Underdatabehandlerne inddeles i tre kategorier, men tilhørende kontrolmetoder:

Høj: Fysisk tilsyn + indhentelse af ekstern revisorerklæring

Mellem: Indhente af ekstern revisorerklæring

Lav: Spørgeskema eller egen erklæring

Der udføres kontrol med underdatabehandlere en gang årligt. Det er procesejerne der er ansvarlige for at der bliver udført kontrol med underdatabehandlere.

Vores underdatabehandler Hetzner er kategoriseret som “mellem”.

Ændring i underdatabehandlere

Hvis databehandleraftalen indeholder en generel godkendelse af databehandlere, bliver kunderne som minimum informeret om ændringer til underdatabehandlere, således at kunden har mulighed for at gøre indsigelse.

Hvis databehandleraftalen foreskriver at kunden skal godkende ændringer i underdatabehandlere, indhentes sådan en godkendelse inden der indgås en aftale med den nye underdatabehandler.

Sikkerhedsbrud

Brud på datasikkerheden er defineret som en hændelse, der resulterer i, at der sandsynligvis er en risiko for, at personoplysninger har mistet fortrolighed, integritet eller tilgængelighed.

Medarbejdere er instrueret i at melde sikkerhedsbrud til it-afdelingen som fører en hændelseslog. It-afdelingen skal, om muligt, have et overblik over hændelsen indenfor 24 timer. It-afdelingen samler i samarbejde med de eventuelt implicerede medarbejdere oplysninger omkring hændelsen.

Brud der vurderes til sandsynligvis at medføre en risiko for, registrerede rettigheder eller frihedsrettigheder anmeldes til kunden/dataansvarlige uden unødig forsinkelse. Anmeldelsen indeholder mindst:

- En beskrivelse af karakteren af bruddet på persondatasikkerheden, herunder hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
- Angivelse af navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes.
- En beskrivelse af de sandsynlige konsekvenser af bruddet på persondatasikkerheden
- En beskrivelse af de foranstaltninger, som den dataansvarlige har truffet eller forslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

Vi assisterer kunden med at melde bruddet til Datatilsynet om nødvendigt.

Behandling af forskellige kategorier af personoplysninger

Berú ApS behandler udelukkende almindelige oplysninger, som billeder og kontaktoplysninger.

Brugeradfærd

Opretholdelse af det ønskede sikkerhedsniveau er afhængig af, at vi alle tager ansvar for informationssikkerheden.

Alle ansatte skal være bekendt med sikkerhedspolitikken og gældende retningslinjer for ønsket adfærd.

Ansættelsesforholdet

Alle medarbejdere har et medansvar for at opretholde det ønskede sikkerhedsniveau i Berú. Alle medarbejdere skal:

- Have et generelt kendskab til informationssikkerhed
- Kende deres ansvar for sikkerheden
- Sikre deres personlige adgangskoder
- Passe på organisationens it-udstyr
- Deltage aktivt i rettelse af fejl, løsning af problemer og forbedringer af sikkerheden
- Rapportere hændelser, der kan indikere brud på sikkerheden

Funktionsadskillelse

Medarbejdere, der har behov for at kunne deploy kode (back-end-udviklere og front-end udviklere), samt den supportansvarlige der konfigurerer løsninger, har adgang til serverne. Andre medarbejdere har ikke adgang.

Sikkerhedsprocedurer før ansættelse

Det sikres, at der er skriftlig dokumentation for at alle ansatte er orienteret og har bekræftet at de forstår og accepterer informationssikkerhedspolitikken samt accepterer vores tavshedspligt.

Ansættelsens ophør

Der er procedurer, der sikrer, at it-aktiver returneres, og at adgange og rettigheder ophører ved ansættelsesforholdets ophør. Ligeledes sikres det at medarbejdere bliver gjort bekendt med deres fortsatte tavshedsforpligtelse.

Styring af netværk og drift

Drift af systemer er udlagt til professionel og certificeret tredjepart. De er valgt på baggrund af deres professionelle tilgang til dette.

Som en forudsætning for hurtig imødegåelse af driftsforstyrrelser, er der etableret procedurer for daglig sikkerhedskopiering (backup). Backup opbevares eksternt på en anden geografisk og sikker lokation, hvor sikkerheden jævnligt kontrolleres. Backup varetages ligeledes af professionel tredjepart.

Eksterne serviceleverandører

Der er procedurer til at overvåge, at eksterne serviceleverandører varetager kontroller, som udføres på vegne af Berú, hensigtsmæssigt og i overensstemmelse med det aftalte.

Skadevoldende programmer (vira, orme, spy- og malware)

Skadevoldende programmer kan sætte hele organisationen ud af drift, og det kan være meget dyrt at rense it-systemerne, hvis de er blevet ramt af et hackerangreb eller en virus. Alt godkendt it-udstyr, der er tilsluttet Berú ApS' netværk har, hvor det er muligt, installeret et aktivt og opdateret antivirusprogrammel, der kan opdage, rense og beskytte mod forskellige former for skadevoldende programmer. Det gælder også eksterne brugere, der tilsluttes netværket via fjernopkobling.

Det kontrolleres løbende, at antivirus er aktivt på arbejdsstationerne, og at signaturfilerne ikke er ældre end én uge.

Servere med kundedata er beskyttet med firewall administreret af underleverandør.

Informationsudveksling

Regler i forbindelse med informationsudveksling af fortrolig information via e-mail og andre elektroniske medier findes i retningslinjen for e-mail.

I forbindelse med ekstern opkobling til Berú ApS' systemer må fortrolige data ikke kopieres, flyttes eller lagres på bærbare medier.

Derudover har alle medarbejdere et ansvar for at beskytte ikke overvåget it-udstyr og bærbare datamedier.

Logning og overvågning

Udviklerne står for logning af vore kritiske systemer. Logningerne foretages med henblik på ved mistanke eller sikkerhedsbrud, at kunne føre disse sikkerhedsrelaterede hændelser tilbage til enkeltpersoner eller identificerbart netværksudstyr.

Overvågning af disk space og at serveren kører foretages af underleverandør.

Administration af brugeradgang

Tildeling, ændring og sletning af brugeradgang til systemer og data sker ud fra arbejdsbetingede behov i overensstemmelse med datas klassifikation. Fysiske adgange og brugerrettigheder til netværk og systemer inddrages, når brugeren ikke længere skal have adgang.

Brugerens ansvar

Alle medarbejdere er ansvarlige for deres personlige adgangskoder, og for at følge vedtagne retningslinjer for password.

Mobilt udstyr og fjernarbejdspladser

Informationssikkerhedspolitikken gælder for alt it-udstyr tilhørende Berú. Retningslinjerne for medarbejdere, som skal overholdes ved brug af mobilt udstyr og hjemmearbejdspladser, er:

- Udstyr skal opbevares betryggende
- Password til computere må ikke oplyses til andre.
- Adgang til Berú ApS' netværk, skal ske via individuelle brugerkonti igennem Berú ApS' VPN.

Kryptering

Berú har vurderet, at der grundet typen af data på vores kundeløsninger ikke anvendes kryptering. Da der højst er tale om personoplysninger af normal karakter krypteres indholdet ikke.

Alle kundesites kører via https, så data sendes i krypteret form for slutbrugere som tilgår informationerne over internettet.

Rapportering af sikkerhedshændelser og svagheder

En væsentlig faktor i informationssikkerhedsarbejdet består i at reagere på hændelser af sikkerhedsmæssig karakter.

Derfor skal sikkerhedsmæssige hændelser rapporteres, og der skal ske opfølgning herpå. Alle medarbejdere har pligt til at rapportere sikkerhedshændelser til adm. direktør Rasmus Rudolf, så sikkerhedshændelserne kan imødegås, inden de udvikler sig. Rapportering af sikkerhedshændelser er beskrevet i retningslinje herfor.

Håndtering af sikkerhedsbrud og forbedringer

Målet og ansvaret for håndtering af sikkerhedsbrud er fastlagt af ledelsen.

Sikkerhedshændelser, fejlhændelser og væsentlige brugeraktiviteter i forhold til 1 og 2 klassificerede systemer skal logges, og uønskede hændelser skal så vidt muligt kunne spores tilbage til en enkeltperson.

Opståede problemer skal håndteres og korrigeres med udgangspunkt i en vurdering af alvoren i problemet. Alvorlige problemer skal analyseres med henblik på løbende forbedringer i informationssikkerheden. Hændelser der har indflydelse på tilgængelighed, skal afklares i overensstemmelse med gældende driftsaftaler (SLA). Driftshændelser, der ikke kan afklares inden for aftalt tid, skal håndteres i overensstemmelse med procedurer for hændelseshåndtering, og de ramte brugere og systemejere informeres.

Hvor der kan komme et retsligt efterspil, skal beviser indsamles, opbevares og præsenteres, så vi kan sikre, at de udgør et fyldestgørende og pålideligt bevismateriale.

Sikkerhedspatches

Underleverandør sikre at servere er sikkerhedsopdateret.

Sårbarhedsscanning

Der skal løbende indhentes informationer om sårbarheder i de anvendte systemer. Der foretages eksterne sårbarhedstest hvert år. Sårbarhederne skal evalueres, og passende foranstaltninger implementeres.

Beredskab, backup og restore

Der er etableret en nødplan for genetabelering af websites. Der foretages løbende backup og restoretest af kundedata.

Komplementerende kontroller

Den dataansvarlige er ansvarlig for følgende:

- egne medarbejdere, herunder adgange disse måtte have.
- oplysningspligten overfor de registrerede.

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.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret, at procedurer er opdateret.	Ingen anmærkninger.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Inspiceret, at behandling af personoplysninger alene foregår i henhold til instruks.	Ingen anmærkninger.
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.	Inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Inspiceret, at den dataansvarlige er underrettet i tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.	Der har ikke været behov for underretninger i perioden.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.1	Databehandleren af etableret aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.	Inspiceret, ved kontrol af databehandleraftaler, at der er etableret de aftalte sikringsforanstaltninger.	Det kan konstateres at backuppen sidst er testet i november 2022 og planlægges testet igen i november 2024. Ingen yderligere anmærkninger.
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.	Inspiceret risikovurderingen, og påset, at den tager udgangspunkt i risici for de registrerede. Inspiceret risikovurderingen og påset, at denne er opdateret i perioden.	Ingen anmærkninger.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Inspiceret informationssikkerhedspolitikken, og påset, at der er taget stilling til anvendelse af antivirus. Inspiceret, at alle servere og lokale computere har installeret antivirus som løbende opdateres.	Ingen anmærkninger.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem en firewall. Inspiceret, at firewall er passende konfigureret.	Ingen anmærkninger.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.5	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Inspiceret, at der foreligger procedurer for begrænsning af brugeres adgang til personoplysninger. Inspiceret, medarbejdernes adgange til systemer og påset at der er et arbejdsbetinget behov.	Ingen anmærkninger.
B.6	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning.	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning.	Ingen anmærkninger.
B.7	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme.	Ingen anmærkninger.
B.8	Der er etableret logning af Windows login. Der er opsat logning af adgang til servere og redaktørinterface.	Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning. Inspiceret, at Windows login er konfigureret og aktiveret. Inspiceret, at logning på redaktørinterface er konfigureret og aktiveret.	Ingen anmærkninger.
B.9	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, er sikret med stærke password.	Inspiceret, at der skal anvendes password for at medarbejdere kan tilgå kundedata.	Ingen anmærkninger.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.10	Ændringer til systemer og databaser følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Inspiceret, at der foreligger formaliserede procedurer for håndtering af relevante opdateringer, patches og sikkerhedspatches. Inspiceret ved udtræk af tekniske sikkerhedsparametre og -opsætninger, at systemer, databaser og netværk er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.	Ingen anmærkninger.
B.11	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Inspiceret, at alle tiltrådte medarbejdere, det seneste år, har fået tildelt de korrekte rettigheder iht arbejdsbetinget behov. Inspiceret, at alle fratrådte medarbejdere, det seneste år, har fået adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt.	Ingen anmærkninger.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
		Inspiceret, at der foreligger dokumentation for regelmæssig - mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.	
B.12	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor autentifikation.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at to-faktor autentifikation anvendes ved tilgang til databaser. Inspiceret, at medarbejdere anvender to-faktor autentifikation ved tilgang til databaser.	Ingen anmærkninger.
B.13	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Ingen anmærkninger.
B.14	Der er etableret formelle procedurer for backup af data, samt udførsel af løbende restore-test.	Inspiceret, at der en procedure for backup af kundedata. Inspiceret, at der er procedure for udførsel af restore-test af backup. Inspiceret, at backup og restore-test er foretaget i henhold til procedurerne herfor.	Det kan konstateres at backuppen sidst er testet i november 2022 og planlægges testet igen i november 2024. Ingen yderligere anmærkninger.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.15	Der er etableret en nødplan for genetablering af website som testes løbende.	Inspiceret, at der foreligger en nødplan for genetablering af websites. Inspiceret, at nødplanen er testet.	Det kan konstateres at backup-delen af nødplanen sidst er testet i november 2022 og planlægges testet igen i november 2024. Ingen yderligere anmærkninger.
B.16	Der foretages en årlig ekstern sårbarhedstest på kundeserveren som inkluderer test af: - Certificate - Protocol Support - Key Exchange - Cipher Strength	Inspiceret, at der en procedure for ekstern sårbarhedstest af kundeservere. Inspiceret, at der er foretaget en sårbarhedstest på kundeservere i perioden.	Ingen anmærkninger.

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	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Forespurgt til, om informationssikkerhedspolitikken er tilgængelig for relevante parter.	Ingen anmærkninger.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Inspiceret, at de etablerede sikkerhedsforanstaltninger der beskrives i informationssikkerhedspolitikken, som minimum, er på niveau med de sikkerhedskrav der stilles i den databehandleraftale med dataansvarlige som har de højeste krav til sikkerhed.	Ingen anmærkninger.
C.3	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Medarbejderne bliver endvidere bedt om at læse informationssikkerhedspolitikken.	Inspiceret, at alle nyansat medarbejder har underskrevet en fortrolighedsaftale. Inspiceret, at alle nyansatte har læst informationssikkerhedspolitikken.	Ingen anmærkninger.

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.4	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages Inspiceret, at alle fratrådte medarbejders rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.	Ingen anmærkninger.
C.5	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	Inspiceret, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt.	Ingen anmærkninger.
C.6	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Inspiceret, at der er blevet udført awareness-træning af relevante medarbejdere i perioden.	Ingen anmærkninger.

Kontrolmål D **Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
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. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Inspiceret, at procedurerne er opdateret.	Ingen anmærkninger.
D.2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: Ved ophør af tjenesterne vedrørende behandling forpligtes databehandleren til, efter den dataansvarliges valg, at slette eller tilbagelevere alle personoplysninger til den dataansvarlige, samt at slette eksisterende kopier, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Ingen anmærkninger.
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Forespurgt til, om der har været ophørte databehandleraftaler i perioden. Inspiceret, at data tilhørende ophørte kunde er blevet slettet.	Ingen anmærkninger.

Kontrolmål E **Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Inspiceret, at procedurerne er opdateret.	Ingen anmærkninger.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder.	Ingen anmærkninger.

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.**			
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. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Ingen anmærkninger
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Inspiceret, at databehandleren kun anvender specifikke eller generelle godkendte underdatabehandlere.	Ingen anmærkninger.
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. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	Ingen anmærkninger.
F.4	Databehandleren har, som minimum, pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Inspiceret, at databehandleren, som minimum, har pålagt underdatabehandleren tilsvarende databeskyttelsesforpligtelser, som dem, der er forudsat i databehandleraftaler med dataansvarlige.	Ingen anmærkninger.

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.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen anmærkninger.
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.	Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende.	Ingen anmærkninger.

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. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at personoplysninger alene overføres til tredjelande eller internationale organisationer i henhold til aftale med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Inspiceret, at procedurerne er opdateret.	N/A – ingen overførsler til tredjelande.

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.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.	Ingen anmærkninger.
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.	Inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.	Ingen anmærkninger.

Kontrolmål I **Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at proceduren er opdateret.	Ingen anmærkninger.
I.2	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 72 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Forespurgt underdatabehandlerne, om de har konstateret nogen brud på persondatasikkerheden i erklæringsperioden.	Ingen anmærkninger.
I.3	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for: • Beskrivelse af karakteren af bruddet på persondatasikkerheden • Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden • Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Ingen anmærkninger.

Kontrolmål I **Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
		Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.	