et trygt samfund med it og data

Revisorerklæring

Berú ApS

ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder for perioden fra 13. december 2019 til 31. januar 2021

REVI-IT A/S | www.revi-it.dk
Højbro Plads 10, 1200 København K
CVR: 30 98 85 31 | Tlf. 33 11 81 00 | info@revi-it.dk
www.dpo-danmark.dk | www.revi-cert.dk

Maj 2021

Indholdsfortegnelse

Afsnit 1: Berú ApS' beskrivelse af behandlingsaktivitet for leverancen af GoBasic

Introduktion

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.

GDPR og Berú ApS' rolle og ansvar som databehandler

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 instruktioner 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 (artikel 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 dataansvarlige 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.

Formål

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 markedsføringsbrug, 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.

Fortegnelse over behandlingsaktiviteter

Der er udarbejdet en elektronisk fortegnelse over behandlingsaktiviteter, som indeholder alle forhold hvor virksomheden behandler personoplysninger på vegne af andre.

Fortegnelsen indeholder som minimum:

- Navn og kontaktoplysninger på os som databehandler og, hvis det er relevant, vores repræsentant og databeskyttelsesrådgiver
- Navn og kontaktoplysninger på alle kunder/dataansvarlige vi behandler data på vegne af og, hvis det er relevant, deres repræsentant og databeskyttelsesrådgiver
- De kategorier af behandling, der foretages på vegne af den enkelte kunde/dataansvarlig
- Hvor det er relevant, overførsler af personoplysninger til et tredjeland eller en international organisation, herunder angivelse af dette tredjeland og beskrivelse af dokumentation for passende garantier
- Hvis det er muligt, en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger

Kontrol:
Der bliver årligt foretaget en gennemgang af fortegnelsen for at sikre, og at den er retvisende.

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.

Privacy by design and by default

Midlertidige filer

Vi sikrer os at midlertidige filer der bliver dannet i forbindelse med behandling af personoplysninger, bliver slettet. Filer med personoplysninger opbevares centralt og medarbejderne er instrueret i løbende at slette disse, når de ikke længere er nødvendige. Der er tilmed etableret ledelseskontroller der skal følge op på om sletningen bliver foretaget.

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. Vi anvender Gmail og deres kryptering (TLS).

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.

Notifikation af videregivelsesforespørgsler

Vi afviser alle henvendelser om videregivelse af vores kunders personoplysninger, som ikke er juridisk bindende.

Vi notificerer kunden hvis vi får juridisk bindende henvendelser om videregivelse af deres personoplysninger og hvis det ikke kræves fra myndighederne, at vi ikke oplyser kunden om det.

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 underdatabehandleren 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 underdatabehandleren 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.

Databeskyttelsesansvarlig (DPO)

Berú ApS har ikke udpeget en DPO, da vi ikke foretager behandling af følsomme personoplysninger eller foretager automatisk overvågning af personer.

Sikkerhed for behandling, anmeldelse og kommunikation

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.

Anvendelse af it og behandling af data er selvfølgelige redskaber i varetagelsen af de daglige arbejdsopgaver. Håndteringen af vore redskaber kræver ikke specielle forudsætninger, men bør ske med omtanke og almindelig sund fornuft.

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.

Uafhængighed af nøglepersoner

Der tilstræbes uafhængighed af enkeltpersoner gennem videndeling og etablering af personbackup, hvor dette er muligt. Hvor videndeling ressourcemæssigt ikke er muligt, skal der etableres relevante kompenserende kontroller, der gør det muligt at udføre opgaverne og sikre den nødvendige dokumentation herfor.

Sikkerhedsprocedurer før ansættelse

Der foretages en aktiv kvalitativ vurdering af ledelsen ifm. ansættelser. Denne vurdering skal sikre ansættelse af kompetente og sikkerhedsmæssigt egnede medarbejdere.

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.

Fysisk sikkerhed

Adgangen til alle fysiske lokaliteter er sikret mod uvedkommendes adgang.

Sikret lokation

Lokaler hos Berú aflåses med alarm og tågesikring, når ingen er til stede.

Fysisk adgangskontrol

Adgang til kontoret tildeles alle medarbejdere. Ved gæstebesøg skal medarbejdere der har inviteret på alle tidspunkter være sammen med gæsten / kunden.

Beskyttelse af udstyr

It-udstyr hos Berú anses ikke som kritisk, da det er dataene der forbindes til som er kritisk. Når it-udstyr bortskaffes eller på anden måde udskiftes, slettes alle data så de ikke kan gendannes.

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.

Operationelle procedurer og ansvarsområder

For at sikre stabiliteten i driften er der etableret funktionsadskillelse, således at test og produktion holdes adskilt på forskellige servere. Nye systemer og ændringer til eksisterende systemer testes inden installering i driftsmiljøet, således at tilgængelighed og integritet sikres. Der er en fast procedure for at kodeændringer med risiko for nedetid altid deployes til testmiljø og testes før der deployes til produktionsmiljøet.

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.

Styring af driftsmiljø

Der er procedurer, der sikrer stabilitet ved installation af systemer i driftsmiljøer. Der anvendes standardopsætninger for konfiguration af systemkomponenter, som kontrollerer kendte sårbarheder.

It-afdelingen skal løbende vurdere tilgængelige sikkerhedsrettelser, f.eks. ”patches” og ”hotfixes” til anvendte operativsystemer. Sikkerhedsrettelser installeres efter behov.

Data, der anvendes til test, skal udvælges omhyggeligt, kontrolleres nøje og beskyttes i henhold til deres klassifikation. Der er særligt fokus på beskyttelse af persondata.

Kapaciteten i forbindelse med alle servere med kritiske informationer skal løbende overvåges for at sikre pålidelig drift og tilgængelighed.

Ved implementering af nye systemer skal det sikres, at der er mulighed for reetablering og fornøden fejlhåndtering.

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.

Netværkssikkerhed

For at undgå uautoriseret adgang, skal vores netværk sikres. Det sker via adgangskontrol og adskillelse af netværkstjenester, hvor dette er hensigtsmæssigt.

Det skal sikres, at it-afdelingen vedblivende har den nødvendige viden samt redskaber til overvågning af Berú ApS' netværk for at kunne opdage og spore sikkerhedsbrister samt til fejlretning. Netværket overvåges løbende med henblik på at opdage og udbedre brud på sikkerheden. Bærbare medier med adgang til netværket skal styres og beskyttes.

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 uovervåget 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 sker kun ved mistanke eller brud på sikkerhed, grundet vores risikovurdering.

Der er internt i Berú aftalt gennemgang af korrekt opsat af logning på hosting-servere hos tredje part i 1. kvartal 2020.

De forretningsmæssige krav til adgangsstyring

Alle informationsaktiver (programmel, udstyr, data, informationer og databærende medier) skal i nærmere specificeret omfang være beskyttet mod uautoriseret adgang.

Ud over den nødvendige adgangskontrol til bygninger og lokaler, anvendes der elektroniske/-programmelbaserede adgangskontrolsystemer. Disse skal ud over adgangskontrol i nødvendigt omfang kunne alarmere og via logning danne grundlag for efterfølgende kontrol.

Der skal løbende tages stilling til adgangsforhold til bygningerne og it-systemerne, og der er retningslinjer og procedurer for tildeling af adgang til bygningernes lokaler med arbejdsstationer, arkiver, netværk og lignende ressourcer.

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 http, så data sendes i krypteret form for slutbrugere som tilgår informationerne over internettet.

Styring af driftsmiljøet

Der er etableret procedurer, der sikrer stabilitet ved installation af systemer i driftsmiljøet.

Data, der anvendes til test, skal udvælges omhyggeligt, kontrolleres nøje og beskyttes i henhold til deres klassifikation.

Berú besidder kildekode til webudvikling. Kildekode opbevares hos tredjepartpart.

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.

Overensstemmelse med lovbestemte krav

Da der er flere lovgivninger, der påvirker vores daglige administration, skal der tages højde for disse i vores informationssikkerhedspolitik og de dertilhørende retningslinjer. Berú ApS' retningslinjer og procedurer skal være i overensstemmelse med alle sikkerhedskrav i lovgivning og med indgåede kontrakter.

Der er procedurer, der sikrer, at relevante sikkerhedskrav i lovgivning, bekendtgørelser samt i indgåede kontraktlige forpligtelser styres og overholdes for de enkelte systemer såvel som for Berú som helhed.

Den fornødne juridiske ekspertise skal inddrages i vurderingen af disse krav.

Væsentlige ændringer i perioden

Der har ikke været væsentlige ændringer i perioden.

Komplementerende kontroller

Den dataansvarlige er ansvarlig for følgende:

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

Afsnit 2: Berú ApS' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for Berú ApS' kunder, som har indgået en databehandleraftale med Berú ApS, 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 ApS anvender underleverandøren og underdatabehandleren Hetzner. Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos Berú ApS' underleverandører og underdatabehandlere.

Berú ApS bekræfter, at:

a) Den medfølgende beskrivelse, afsnit 1, giver en retvisende beskrivelse af, hvordan Berú ApS har behandlet personoplysninger på vegne af dataansvarlige i perioden fra den 13. december 2019 til 31. januar 2021 Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan Berú ApS' 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 GoBasics 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 ydelse GoBasic til behandling af personoplysninger foretaget i hele perioden fra den 13. december 2019 til 31. januar 2021

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne ydelse GoBasic, 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 GoBasic, 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 13. december 2019 til 31. januar 2021. 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 13. december 2019 til 31. januar 2021

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, den 17. maj 2021
Berú ApS

Rasmus Rudolf
Managing Partner

Afsnit 3: Uafhængig revisors erklæring med høj grad af sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder om i perioden fra den 13. december 2019 til 31. januar 2021

Til Berú ApS, Berú ApS' kunder i rollen som dataansvarlige og disses revisorer.

Omfang

Vi har fået som opgave at afgive erklæring med høj grad af sikkerhed om Berú ApS' beskrivelse i "Afsnit 1" af GoBasic i henhold til databehandleraftaler med deres kunder, i rollen som dataansvarlig i perioden fra den 13. december 2019 til 31. januar 2021 og b+c om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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

Vores konklusion udtrykkes med høj grad af sikkerhed.

Berú ApS' ansvar

Berú ApS er ansvarlig for udarbejdelsen af beskrivelsen og 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 samt for at udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i såvel IESBA's Etiske regler som FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), som er baseret på de grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

REVI-IT A/S anvender international standard om kvalitetsstyring, ISQC 1[1] , og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder og gældende krav ifølge lovgivning og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Berú ApS' 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, med henblik på at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er

[1] ISQC 1, Kvalitetsstyring i firmaer, som udfører revision og review af regnskaber, andre erklæringsopgaver med sikkerhed og beslægtede opgaver.

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 GoBasic samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i "Afsnit 1".

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

Begrænsninger i kontroller hos en databehandler

Berú ApS' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved GoBasic, 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 GoBasic, således som denne var udformet og implementeret i perioden fra den 13. december 2019 til 31. januar 2021, 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 13. december 2019 til 31. januar 2021, 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 13. december 2019 til 31. januar 2021.

Beskrivelse af test af kontroller

De specifikke kontroller, der er testet, samt arten og resultater af disse tests, fremgår i afsnit 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i det efterfølgende afsnit, Afsnit 4, er udelukkende tiltænkt dataansvarlige, der har anvendt Berú ApS' GoBasic, 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 17. maj 2021

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Christian H. Riis
Partner, CISA

Afsnit 4: Kontrolmål, udførte kontroller, test og resultater heraf

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

Vores test af funktionaliteten har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår af kontrolmålene A-J nedenfor. Vores test har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte kontrolmål blev nået i perioden fra den 13. december 2019 til 31. januar 2021].

Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos Berú ApS' underleverandører og underdatabehandlere.

Kontroller udført hos de dataansvarlige er ikke omfattet af vores erklæring.

Vi har udført vores tests af kontroller hos Berú ApS via følgende handlinger:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af passende personale hos Berú ApS. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Observation af, hvordan kontroller udføres
Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres.
Genudførelse af kontrol	Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

Kortlægning af kontrolområder op mod GDPR-artikler, ISO 27701 og ISO 27001/2

I tabellen nedenfor er kontrolaktiviteterne i den følgende oversigt kortlagt op mod artiklerne i GDPR, samt mod ISO 27701 og ISO 27001/2.

Artikler og punkter markeret med fed angiver primære områder.

Kontrolaktivitet	GDPR-artikler	ISO 27701	ISO 27001/2
A.1	5, 26, **28**, 29, 30, 32, 40, 41, 42, 48	8.5.5, 5.2.1, 6.12.1.2, 6.15.1.1, 8.2.1, **8.2.2**	*Nyt område ift. ISO 27001/2*
A.2	**28**, 29, 48	8.5.5, 6.15.2.2, **6.15.2.2**	18.2.2
A.3	**28**	**8.2.4, 6.15.2.2**	18.2.2
B.1	31, **32**, 35, 36	**5.2.2**	4.2
B.2	**32,** 35, 36	**7.2.5, 5.4.1.2, 5.6.2**	6.1.2, 5.1, 8.2
B.3	**32**	**6.9.2.1**	**12.2.1**
B.4	28 stk. 3; litra e, **32; stk. 1**	**6.10.1.1, 6.10.1.2, 6.10.1.3**, 6.11.1.3	**13.1.2**, 13.1.3, 14.1.3, 14.2.1
B.5	32	6.6.1.2, 6.10.1.3	9.1.2, 13.1.3, 14.2.1
B.6	**32**	**6.6**	9.1.1, 9.2.5
B.7	**32**	**6.9.4**	12.4
B.8	**32**	**6.15.1.5**	18.1.5
B.9	**32**	**6.9.4**	12.4
B.10	**32**	**6.11.3**	14.3.1
B.11	**32**	**6.9.6.1**	12.6.1
B.12	28, **32**	**6.9.1.2, 8.4**	12.1.2
B.13	**32**	**6.6**	9.1.1
B.14	**32**	**7.4.9**	*Nyt område ift. ISO 27001/2*
B.15	**32**	**6.8**	11.1.1-6
C.1	**24**	**6.2**	5.1.1, 5.1.2
C.2	**32, 39**	**6.4.2.2, 6.15.2.1, 6.15.2.2**	7.2.2, 18.2.1,18.2.2
C.3	**39**	**6.4.1.1-2**	7.1.1-2
C.4	28, 30, **32, 39**	**6.10.2.3**, 6.15.1.1, 6.4.1.2	7.1.2, 13.2.3
C.5	**32**	**6.4.3.1, 6.8.2.5, 6.6.2.1**	7.3.1, 11.2.5, 8.3.1
C.6	**28,** 38	**6.4.3.1, 6.10.2.4**	7,3.1, 13.2.4
C.7	**32**	**5.5.3, 6.4.2.2**	7.2.2, 7.3
C.8	**38**	**6.3.1.1, 7.3.2**	6.1.1
C.9	6, 8, 9, 10, 15, 17, 18, 21, 28, **30**, 32, 44, 45, 46, 47, 48, 49	6.12.1.2, 6.15.1.1, 7.2.2, **7.2.8**, 7.5.1, 7.5.2, 7.5.3, 7.5.4, **8.2.6**, 8.4.2, 8.5.2, 8.5.6	*Nyt område ift. ISO 27001/2*
D.1	6, 11, **13, 14,** 32	**7.4.5**, **7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
D.2	6, 11, 13, 14, **32**	**7.4.5**, **7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
D.3	13, **14**	**7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
E.1	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*Nyt område ift. ISO 27001/2*
E.2	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*Nyt område ift. ISO 27001/2*
F.1	6, 8, 9, 10, 17, 18, 22, 24, 25, 28, **32,** 35, 40, 41, 42	5.2.1, **7.2.2**, **7.2.6**, 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7	15
F.2	**28**	**8.5.7**	15
F.3	**28**	**8.5.8**, 8.5.7	15
F.4	**33, 34**	**6.12.1.2**	15
F.5	**28**	**8.5.7**	15
F.6	**33, 34**	**6.12.2**	15.2.1-2
G.1	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, **8.5.1**, 8.5.2, 8.5.3	13.2.1, 13.2.2

G.2	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1,** 7.5.2, 7.5.3, 7.5.4, **8.4.2,** 8.5.2, 8.5.3	13.2.1
G.3	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
H.1	12, **13, 14,** 15, 20**,** 21	**7.3.5, 7.3.8, 7.3.9**	*Nyt område ift. ISO 27001/2*
H.2	12, **13, 14,** 15, 20**,** 21	**7.3.5, 7.3.8, 7.3.9**	*Nyt område ift. ISO 27001/2*
I.1	**33, 34**	**6.13.1.1**	16.1.1-5
I.2	**33, 34**, 39	6.4.2.2, **6.13.1.5, 6.13.1.6**	16.1.5-6
I.3	**33, 34**	**6.13.1.4**	16.1.5
I.4	**33, 34**	**6.13.1.4,** 6.13.1.6	16.1.7

Kontrolmål A – Instruks vedrørende behandling af personoplysninger

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

Nr.	*Berú ApS' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af 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.	Vi har inspiceret Informationssikkerhedspolitikken og påset, at der foreligger procedurer for at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Vi har inspiceret, at politikken er opdateret.	Ingen afvigelser konstateret.
A.2	Databehandleren udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at databehandleren alene udfører den behandling, som fremgår af instruksen.	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.	Vi har inspiceret informationssikkerhedspolitikken, og påset, at der er taget stilling til ulovlige instrukser fra dataansvarlige. Vi har forespurgt, om der har været instrukser i perioden, som Berú har vurderet som ulovlige.	Vi er blevet informeret om, at der ikke har været instrukser i perioden, som Berú har vurderet til at være ulovlige, hvorfor vi ikke har kunnet teste effektiviteten af deres procedurer. Ingen afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	*Berú ApS' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af test*
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at de aftalte sikkerhedsforanstaltninger etableres. Vi har inspiceret, at procedurerne er opdaterede.	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.	Vi har inspiceret risikovurderingen, og påset, at den tager udgangspunkt i risici for de registrerede. Vi har inspiceret risikovurderingen og påset, at denne er opdateret i perioden.	Ingen afvigelser konstateret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Vi har inspiceret informationssikkerhedspolitikken, og påset, at der er taget stilling til anvendelse af antivirus. Vi har stikprøvevis inspiceret servere og lokale computere, og påset, at der er installeret antivirus som løbende opdateres.	Ingen afvigelser konstateret.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Vi har stikprøvevis inspiceret firewall konfiguration, og stikprøve påset, at dette er konfigureret i henhold til intern politik.	Ingen afvigelser konstateret.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Vi har inspiceret, at der foreligger procedurer for begrænsning af brugeres adgang til personoplysninger. Vi har stikprøvevis inspiceret adgange, og stikprøvevis påset, at der er et arbejdsbetinget behov.	Ingen afvigelser konstateret.

Nr.	Berú ApS' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Vi har inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering. Vi har stikprøvevist inspiceret, at der er sket opfølgning på alarmer, samt at forholdet er meddelt de dataansvarlige i behørigt omfang.	Ingen afvigelser konstateret.
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Vi 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. Vi har inspiceret, at teknologiske løsninger til kryptering har været tilgængelige og aktiveret i hele erklæringsperioden. Vi har inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail. Vi har forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger i erklæringsperioden, samt om de dataansvarlige er behørigt orienteret herom.	Ingen afvigelser konstateret.
B.9	Der er etableret logning af Windows login.	Vi har inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang og opfølgning på logs. Vi har inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret. Vi har inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning.	Ingen afvigelser konstateret.

Nr.	Berú ApS' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
		Vi har stikprøvevist inspiceret, at logfiler har det forventede indhold i forhold til opsætning, og at der er dokumentation for den foretagne opfølgning og håndtering af evt. sikkerhedshændelser. Vi har stikprøvevist inspiceret, at der er dokumentation for den foretagne opfølgning på aktiviteter udført af systemadministratorer og andre med særlige rettigheder.	
B.11	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, er sikret med stærke password.	Vi har stikprøvevis inspiceret anvendelse af passwords, og stikprøvevis påset, at disse medarbejdere har opdateret deres password.	Ingen afvigelser konstateret.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Vi har inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Vi har 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 afvigelser konstateret.
B.13	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.	Vi har inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Vi har stikprøvevist inspiceret, at medarbejderes adgange til systemer og databaser er godkendt, og at der er et arbejdsbetinget behov. Vi har stikprøvevist inspiceret, at fratrådte medarbejdere adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Vi har inspiceret, at der foreligger dokumentation for regelmæssig - mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.	Ingen afvigelser konstateret.

Nr.	Berú ApS' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
B.14	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.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at to-faktor autentifikation anvendes ved behandling af personoplysninger, der medfører højrisiko for de registrerede. Vi har inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører høj-risiko for de registrerede, alene kan ske ved anvendelse af to-faktor autentifikation.	Ingen afvigelser konstateret.
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Vi har 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. Vi har inspiceret dokumentation for, at kun autoriserede personer har haft fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger, i erklæringsperioden.	Ingen afvigelser konstateret.

Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	Berú ApS' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af 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.	Vi har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Vi har forespurgt til, om informationssikkerhedspolitikken er tilgængelig for relevante parter.	Ingen afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at aftalerne ikke er i modstrid med informationssikkerhedspolitikken.	Ingen afvigelser konstateret.

Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	*Berú ApS' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af test*
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Vi har stikprøvevis inspiceret listen over ansættelser i perioden, og stikprøvevis forespurgt, om der har været efterprøvning af nyansatte i perioden.	Ingen afvigelser konstateret.
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	• Vi har stikprøvevis inspiceret ansættelser i perioden, og stikprøvevis inspiceret, at de har underskrevet fortrolighedsaftaler.	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.	Vi har inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder deaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages. Vi har stikprøvevis inspiceret listen over fratrådte medarbejdere i perioden, og stikprøvevis påset, at adgange og aktiver er blevet inddraget.	Ingen afvigelser konstateret.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Vi har stikprøvevis inspiceret listen over fratrådte medarbejdere i perioden, og stikprøvevis påset, at de er blevet orienteret omkring fortroligheden.	Ingen afvigelser konstateret.

Nr.	Berú ApS' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
C.7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har forespurgt til, om der er blevet udført awareness-træning af medarbejdere i perioden.	Ingen afvigelser konstateret.
C.8	Databehandleren har vurderet behovet for en DPO, og har sikret, at DPO'en har tilstrækkelig faglighed til at udføre sine opgaver, samt at DPO'en bliver inddraget i relevante områder.	Vi har inspiceret, at databehandleren har foretaget en vurdering af om denne har pligt til at udpege en DPO.	Ingen afvigelser konstateret.
C.9	Der foreligger hos databehandleren en fortegnelse over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om fortegnelsen skal opdateres.	Vi har inspiceret, at der foreligger fortegnelser, som ledelsen har behandlet og godkendt inden for det seneste år.	Ingen afvigelser konstateret.

Kontrolmål D -Tilbagelevering og sletning af personoplysninger

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

Nr.	Berú ApS' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af 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.	Vi har inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
D.2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Vi har stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at der er aftalt krav til opbevaring og sletterutiner.	Ingen afvigelser konstateret.

Kontrolmål D -Tilbagelevering og sletning af personoplysninger

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

Nr.	*Berú ApS' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af test*
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.	Vi har forespurgt til, om der har været ophørte databehandleraftaler i perioden.	Vi her blevet informeret om, at der ikke har været ophørte databehandleraftaler i perioden, hvorfor vi ikke har kunnet teste effektiviteten af databehandlerens procedurer. Ingen afvigelser konstateret.

Kontrolmål E – Opbevaring af personoplysninger

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

Nr.	*Berú ApS' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af 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 skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Vi har inspiceret, at proceduren er opdateret.	Ingen afvigelser konstateret.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Vi har inspiceret, at databehandleren kun anvender godkendte lokaliteter til databehandling og opbevaring.	Ingen afvigelser konstateret.

Kontrolmål F – Anvendelse af underdatabehandlere

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

Nr.	*Berú ApS' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af 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.	Vi har inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Vi 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.	Vi har stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at databehandler kun anvender specifikke eller generelle godkendte underdatabehandlere.	Ingen afvigelser konstateret.
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.	Vi har inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Vi har stikprøvevis inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	Ingen afvigelser konstateret.
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har stikprøvevis påset, at databehandleren har pålagt samme eller tilsvarende databeskyttelsesforpligtelser, som dem, der er forudsat i databehandleraftaler med dataansvarlige.	Ingen afvigelser konstateret.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere.	Vi har stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at disse indeholder en samlet oversigt over underdatabehandlere.	Ingen afvigelser konstateret.

Nr.	Berú ApS' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af test
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.	Vi har inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Vi har inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Vi har inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende.	Ingen afvigelser konstateret.

Kontrolmål G – Overførsel af personoplysninger til tredjelande

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.	Berú ApS' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat af 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.	Vi har inspiceret informationssikkerhedspolitikken, og påset, at der er taget stilling til overførsel til tredjelande. Vi har stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at der er taget stilling til tredjelandsoverførsler. Vi har forespurgt til, om databehandleren overfører persondata til tredjelande.	Vi er blevet informeret om, at databehandleren ikke overfører til tredjelande, og vi finder det sandsynliggjort på baggrund af vores testhandlinger. Ingen afvigelser konstateret.

Kontrolmål I – Håndtering af persondatasikkerhedsbrud

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

Nr.	*Berú ApS' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat af 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.	Vi har inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Vi har inspiceret, at proceduren er opdateret.	Ingen afvigelser konstateret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Vi har stikprøvevis inspiceret brud i perioden, og stikprøvevis påset, at dataansvarlige er blevet rettidig underrettet.	Ingen afvigelser konstateret.
I.4	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.	Vi har inspiceret procedurer for håndtering af sikkerhedsbrud, og påset, at disse sikrer bistand til de dataansvarlige i forbindelse med brud. Vi har stikprøvevis inspiceret sikkerhedsbrud i perioden, og stikprøvevis påset, at dataansvarlige har fået relevant bistand.	Ingen afvigelser konstateret.