Erklæring fra uafhængig revisor

Erklæringsafgivelse i forbindelse med overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov for leverancen af GoBasic pr. 12. december 2019

ISAE 3000

Berú ApS

CVR-nr.: 35 24 25 89

December 2019

Indholdsfortegnelse

Berú ApS' udtalelse

Denne erklæring vedrører Berú ApS' overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov.

Vi bekræfter, at vi, efter vores opfattelse, i al væsentlighed har overholdt ovennævnte kriterier, pr. 12-12-2019.

Vi bekræfter herudover, at revisor har haft adgang til al information og materiale, som har været nødvendig for erklæringsafgivelsen.

På den baggrund er det vores vurdering, at vi, i al væsentlighed, har udført en hensigtsmæssig drift og administration for vores ydelser.

København, 12. december 2019

Berú ApS

Rasmus Rudolf
Managing Partner

Berú ApS' kontrolbeskrivelse af tjenesten GoBasic samt interne kontroller

Introduktion

Formålet med denne beskrivelse er at levere oplysninger til Berú ApS' kunder og deres interessenter (herunder revisorer) om kravene og indholdet af EU' s Generelle Databeskyttelsesforordning ("GDPR").
Desuden er 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 en række underdatabehandlere til hosting af servere, herunder Wannafind.dk og Hetzner, som begge er ISO 27001 certificeret.

Risikostyring i Berú ApS

BerúApS 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 to underdatabehandlere Hetzner og Wannafind er begge 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

Størstedelen af medarbejderne har adgang til serverne, da dette er påkrævet i det daglige arbejde med at supportere kunder. De medarbejdere som sidder med filmproduktion, har dog ikke adgang til serverne.

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 Berús 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 anti-virus er aktivt på arbejdsstationerne, og at signatur-filerne 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 Berús 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 Berús 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 Berús netværk, skal ske via individuelle brugerkonti igennem Berús 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. Berús 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.

Uafhængig revisors erklæring om overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov pr. 12-12-2019

Til Berú ApS' ledelse, selskabets kunder og disses revisorer.

Vi har efter aftale undersøgt Berú ApS' overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov pr. 12-12-2019.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Erklæringen er alene udarbejdet til brug for Berú ApS' ledelse, selskabets kunder og disses revisorer til vurdering af de tilrettelagte forretningsgange, og kan ikke anvendes til andre formål.

Ledelsens ansvar

Ledelsen i Berú ApS har ansvaret for at implementere og sikre opretholdelsen af forretningsgange som kræ-vet af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov.

Revisors ansvar

Det er vores ansvar, på grundlag af det udførte arbejde, at udtrykke en konklusion om, hvorvidt selskabet overholder de krav, der er nævnt i databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov.

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 revisorlovgiv-ning med henblik på at opnå høj grad af sikkerhed for vores konklusion.

REVI-IT A/S er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender således et omfat-tende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende krav i lov og øvrig regulering.

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 integri-tet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

Vores arbejde har omfattet forespørgsler, observationer samt vurdering og stikprøvevis undersøgelse af den information, vi har modtaget.

På grund af begrænsninger i ethvert kontrolsystem kan der opstå fejl eller besvigelser, som ikke afdækkes af vort arbejde. Endvidere vil en anvendelse af vor konklusion på efterfølgende perioders transaktioner være undergivet en risiko for, at der foretages ændringer af systemer eller kontroller, ændring i kravene til be-handling af oplysninger eller i selskabets overholdelse af de beskrevne politikker og procedurer, hvorved vores konklusion eventuelt ikke længere vil være gældende.

Begrænsninger i kontroller hos en dataansvarlig

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 de-res art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. Herudover er fremskrivnin-gen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

Konklusion

Denne konklusion er udformet på grundlag af forståelsen af de kriterier, som der er redegjort for i erklæringens indledende afsnit, og som bygger på kravene i databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov**.**

Det er vores opfattelse, at Berú ApS, i alle væsentlige henseender, lever op til ovennævnte kriterier, pr. 12. december 2019.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt kunder, der har anvendt Berú ApS' ydelser, og deres revisorer, som har en tilstrækkelig kompetence til at vurdere den medfølgende beskrivelse sammen med anden information, herunder information om kunders egne kontroller.

København, 12. december 2019

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Martin Brogaard Nielsen
It-revisor, CISA, CIPP/E, CRISC, adm. direktør

Kontrolmål, udførte kontroller, test og resultater heraf

Den følgende oversigt er udformet for at skabe et overblik over de kontroller, som Berú ApS har implementeret i henhold til overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov. Vores test af funktionaliteten har omfattet de kontroller, som vi har vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte artikler pr. 12. december 2019 er efterlevet.

De krav, som fremgår direkte af forordningen eller loven, kan ikke fraviges. Derimod kan der justeres på, hvordan sikkerheden implementeres, da sikkerhedskravene i forordningen på flere punkter er af mere generel og overordnet karakter, som bl.a. skal tage hensyn til formål, behandlingens karakter, kategorien af personoplysninger mv. Herudover kan der være konkrete krav i de enkelte kundekontrakter, der kan have en rækkevidde, der går ud over databeskyttelseslovens almindelige krav. Disse er i givet fald ikke omfattet af nedenstående.

Kontroller udført hos Berú ApS' kunder er herudover ikke omfattet af vores erklæring, idet kundernes egne revisorer må foretage denne gennemgang og vurdering.

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

Metode	Overordnet beskrivelse
Forespørgsel	Interview, altså forespørgsel af udvalgt personale hos virksomheden angående kontroller
Observation	Observation af, hvordan kontroller udføres
Inspektion	Gennemgang og stillingtagen til politikker, procedurer og dokumentation vedrørende kontrollers udførelse
Genudførelse af kontrol	Vi har selv udført – eller har observeret – en genudførelse af kontroller med henblik på at verificere, at kontrollen fungerer som forventet

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.	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 én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger procedurer for at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Inspiceret, at proceduren er opdateret.	Ingen væsentlige afvigelser konstateret.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har inspiceret, at den behandling der foretages svarer til instruksen i databehandleraftaler med dataansvarlige.	Ingen væsentlige 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, at der foreligger en procedure for underretning af dataansvarlige hvis en instruks er i strid med lovgivningen.	Ingen væsentlige 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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors 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 én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Vi har inspiceret, at proceduren er opdateret.	Ingen væsentlige 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, at der foreligger en risikovurdering. Vi har inspiceret, at implementerede tekniske og organisatoriske foranstaltninger er i overensstemmelse med den foretagende risikovurdering.	Ingen væsentlige afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Vi har inspiceret, at der er installeret antivirus på alle relevante systemer og databaser.	Det er konstateret at én ud af tre kundeservere har opdateret antivirus. De to resterende er under opgradering og vil blive opdateret med MS antivirus når opgraderingen er udført.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Vi har inspiceret, at der er installeret firewall på alle relevante systemer og databaser.	Ingen væsentlige afvigelser konstateret.
B.5	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Vi har inspiceret, at adgange til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Ingen væsentlige afvigelser konstateret.
B.6	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter:) Ping test	Vi har inspiceret, at der er etableret relevant systemovervågning for systemer og databaser der benyttes til behandling af personoplysninger.	Ingen væsentlige afvigelser konstateret.
B.7	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Vi har inspiceret, at der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Ingen væsentlige afvigelser konstateret.
B.8	Der er etableret logning på Windows login.	Vi har inspiceret, at der er etableret logning i Windows login.	Ingen væsentlige afvigelser konstateret.
B.9	Ændringer til systemer og databaser følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Vi har inspiceret, at der er opdaterede, sikkerhedspatches på systemer og databaser.	Ingen væsentlige afvigelser konstateret.
B.10	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 proceduren for oprettelse og nedlæggelse af brugere. Vi har inspiceret, at oprettede brugere er oprettet iht. proceduren. Vi har inspiceret, at fratrådte medarbejderes brugere er nedlagt.	Det er konstateret, at der ikke en procedure for oprettelse af brugere grundet organisationens størrelse, er det altid direktøren der opretter alle brugere og tildeler rettigheder.
B.11	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, er sikret med stærke password.	Vi har inspiceret, at der er passende passwordsikkerhed til systemer og databaser hvori der sker behandling af personoplysninger.	Det er konstateret, at gamle passwords kan genbruges. Det anbefaler at password historikken sættes til minimum 5.
B.12	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler, hvori der opbevares og behandles personoplysninger.	Vi har inspiceret, at kontoret er sikret med indbrudsalarmer og låse.	Ingen væsentlige 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.	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. Informationssikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst én gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Vi har inspiceret, at der foreligger en informationssikkerhedspolitik. Vi har inspiceret, at informationssikkerhedspolitikken er delt med relevante interessenter. Vi har inspiceret, at informationssikkerhedspolitikken er opdateret.	Ingen væsentlige afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har inspiceret, at sikkerhedsniveauet i informationssikkerhedspolitikken som minimum svarer til sikkerhedsniveauet i indgåede databehandleraftaler.	Ingen væsentlige afvigelser konstateret.
C.3	Der udføres en efterprøvning af databehandlerens relevante medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: - Referencer fra tidligere ansættelser - CV - Eksamensbeviser	Vi har forespurgt, om der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Ingen væsentlige 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 inspiceret, at ansættelseskontrakter indeholder et afsnit om fortrolighed.	Ingen væsentlige 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, at der er implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Ingen væsentlige afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
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 medarbejderne, ved fratrædelse, oplyses om, at deres fortrolighedsforpligtelse stadig er gældende.	Det er konstateret at der endnu ikke findes en procedure herfor, da der ikke har været fratrædelser i flere år, men ledelsen oplyser at dette vil blive implementeret ved næste fratrædelse.
C.7	Der gennemføres løbende awarenesstræning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har inspiceret, at der er foretaget awarenesstræning af medarbejdere i relation til it-sikkerhed og behandling af personoplysninger.	Ingen væsentlige 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 og 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 væsentlige 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.	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 én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den data-ansvarlige. Vi har inspiceret, at proceduren er opdateret.	Ingen væsentlige afvigelser konstateret.
D.2	Der er aftalt 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.	Vi har inspiceret, at databehandleraftaler indeholder specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Ingen væsentlige afvigelser konstateret.
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 inspiceret, at databehandleren har slettet og/eller tilbageleveret data iht. aftalen med den dataansvarlige.	Ingen væsentlige 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.	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 én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har 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 væsentlige 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 væsentlige 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.	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 én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Vi har inspiceret, at proceduren er opdateret.	Ingen væsentlige afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Vi har inspiceret, at databehandleren alene anvender underdatabehandlere som er specifikt eller generelt godkendt af den dataansvarlige.	Ingen væsentlige afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Vi har inspiceret, at der foreligger en procedure for underretning af dataansvarlige ved ændringer i godkendte underdatabehandlere. Vi har inspiceret, at databehandleren har underrettet den dataansvarlige ved ændringer i underdatabehandlere.	Ingen væsentlige 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 inspiceret, at databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Ingen væsentlige afvigelser konstateret.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: - Navn - CVR-nr. - Adresse - Beskrivelse af behandlingen.	Vi har inspiceret, at databehandleren har en oversigt over godkendte underdatabehandlere,	Ingen væsentlige afvigelser konstateret.
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 er udført kontrol med underdatabehandlere, baseret på en risikovurdering.	Ingen væsentlige 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.	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 én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger skriftlige procedurer, som indeholder krav om, at data-behandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Vi har inspiceret, at proceduren er opdateret.	Ingen væsentlige afvigelser konstateret.

Kontrolmål H – Håndtering af persondatasikkerhedsbrud

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
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Vi har inspiceret, at proceduren er opdateret.	Ingen væsentlige afvigelser konstateret.
H.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: - Awareness hos medarbejdere - Overvågning af servertilgængelighed.	Vi har inspiceret, at databehandleren har etableret awareness træning hos medarbejderne til identificering af brud på sikkerheden. Vi har inspiceret, at databehandleren har etableret ping overvågning af servere.	Ingen væsentlige afvigelser konstateret.
H3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 24 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Vi har inspiceret, at databehandleren har underrettet den dataansvarlige uden unødig forsinkelse ved brud på persondatasikkerheden.	Ingen væsentlige afvigelser konstateret.
H.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, at databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet.	Ingen væsentlige afvigelser konstateret.

Kontrolmål I – Fortegnelse over behandlingsaktiviteter

Der efterleves procedurer og kontroller, som sikrer, at databehandleren fører en fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af de dataansvarlige.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
I.1	Der foreligger hos databehandleren en fortegnelse over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige, som indeholder: - Navn på og kontaktoplysninger for databehandleren for hver dataansvarlig og – hvis det er relevant – den dataansvarliges databeskyttelsesrådgiver - De kategorier af behandling, der foretages på vegne af den enkelte dataansvarlige - Overførsler af personoplysninger til et tredjeland eller en international organisation, og i tilfælde af overførsler i henhold til artikel 49, stk. 1, andet afsnit, dokumentation for passende garantier - En generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger.	Vi har inspiceret, at databehandleren har en fortegnelses over behandlingsaktiviteterne, som indeholder de lovpligtige informationer.	Ingen væsentlige afvigelser konstateret.
I.2	Der foretages løbende – og mindst én gang årligt – vurdering af, hvorvidt fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige skal opdateres.	Vi har inspiceret, at fortegnelsen er opdateret og løbende gennemgås.	Ingen væsentlige afvigelser konstateret.
I.3	Ledelsen har sikret, at fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige er fyldestgørende, opdateret og korrekt.	Vi har inspiceret, at ledelsen har godkendt fortegnelsen.	Ingen væsentlige afvigelser konstateret.