Erklæring fra uafhængig revisor

Erklæringsafgivelse i forbindelse med overholdelse af databeskyttelsesforordningen (GDPR) pr. 17. december 2018

ISAE 3000

HeroBase A/S

CVR-nr.: 31 07 31 03

December 2018

Indholdsfortegnelse

HeroBase A/S' udtalelse

Denne erklæring vedrører HeroBase A/S' overholdelse af databeskyttelsesforordningen (GDPR).

Vi bekræfter, at vi, efter vores opfattelse, i al væsentlighed har overholdt ovennævnte kriterier pr. 17. december 2018.

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.

Søborg, 17. december 2018

HeroBase A/S

Casper Langhoff
Adm. direktør

Kenny Andreasen
CTO & CIO

HeroBase A/S' systembeskrivelse af løsningen Hero Outbound samt interne kontroller

Introduktion

Formålet med denne beskrivelse er at levere information til HeroBases kunder og deres interessenter (herunder revisorer) vedrørende kravene og indholdet i databeskyttelsesforordningen ("GDPR"), beskrevet ud fra rammerne givet i den internationale revisionsstandard ISAE3000, herunder også standarden for erklæringsopgaver om kontroller hos en serviceleverandør, ISAE3402.

Beskrivelsen har herudover det formål at give specifik information om forhold vedrørende behandlingssikkerked, tekniske og organisatoriske foranstaltninger, ansvar mellem dataansvarlige (vores kunder) og databehandler (HeroBase), og hvordan løsningen Hero Outbound gennem funktioner til bl.a. understøttelse af datasubjekternes rettigheder, understøtter vores kunder (de dataansvarlige) i at leve op til GDPR, for så vidt angår deres aktiviteter i Hero Outbound. Det beskrevne er altså gældende for vores leverance af produktet og ydelsen Hero Outbound til vores kunder.

Beskrivelsen omfatter de forhold vedrørende Hero Outbound, som omfatter størstedelen af vores kunder og er baseret på vores standardleverance. Individuelle kundeforhold er ikke medtaget i denne beskrivelse.

HeroBase og vores software Hero Outbound

HeroBase er en dansk IT-virksomhed med base i Søborg. Vi udvikler, hoster og leverer software til kontaktcentre som en SaaS-løsning. Vores kerneprodukt er leverance af softwaren Hero Outbound, der leveres som SaaS-løsning, dvs. er hostet i egne datacentre og bygget op omkring en fleksibel og skalérbar abonnementsbaseret model.

Hero Outbound, som denne erklæring går på, er i øjeblikket det største produkt i vores palette af løsninger samlet under *Hero*-brandet. Andre løsninger indbefatter bl.a. marketing automation platformen Hero Flows, og rådgivnings- og salgstræningsorganet Hero Academy. Hero er valgt som paraplybetegnelse, fordi vi med vores løsninger gerne vil appellere direkte til slutbrugerne af vores software; for Hero Outbounds vedkommende betyder det mestendels brugerne og medarbejderne – også kaldet agenterne – i kontaktcentre – også kaldet callcentre. Vi vil ved at levere en hurtig, intuitiv, effektiv og personlig platform være det foretrukne valg blandt "hverdagens helte", som agenterne i kontaktcentrene omtales som internt i HeroBase.

Vi skaber fundamentet for det mest effektive kontaktcenter

Navnet Hero Outbound er valgt til den løsning, som i øjeblikket er den bærende, fordi den først og fremmest fokuserer på opsøgende salg/rådgivningsarbejde, også kaldet outbound telemarketing. Telemarketing er, om end termen til tider behæftes med en negativ association, fortsat en uhyre effektiv kontaktkanal, fordi den giver mulighed for at dyrke den personlige kontakt mellem agent og personen i "den anden ende af røret". Salgs- og kundekontakter, som starter med opsøgende salg, er dog ingenlunde afgrænset til outbound telemarketing alene. E-mails og SMS'er ligger i naturlig forlængelse af den telefoniske dialog – enten i forbindelse med digital ordreaccept, udsendelse af opfølgende information, koordinationsarbejde o. lign. Hero Outbound muliggør tillige at indgående telefonopkald besvares "blandet" med de udgående telefonopkald – typisk når der ringes tilbage fra personer, som har et ubesvaret opkald på deres telefon, eller i forbindelse med indgående salgshenvendelser affødt af kampagner o. lign.

Hero Outbound kan således, selv uden produkter fra den øvrige palette af Hero-løsninger, for mange kontaktcentre udgøre den eneste nødvendige software, centret skal bruge til at udføre sine aktiviteter blandt

agenterne (salg, mødebooking, fundraising, meningsmålinger o.m.a.) og blandt ledere og administratorer, som tilrettelægger og monitorerer agenternes arbejde.

Disse "aktiviteter" indbefatter også selve handlingen at ringe ud eller besvare telefonen. Som webapplikation betjenes Hero Outbound fra en browser, og med et headsæt tilsluttet til computeren kan telefonopkald udføres og besvares via den indbyggede samtaleteknologi Hero Phone, som er baseret på WebRTC-frameworket. Hermed er ingen eksterne telefoner eller tredjepartsløsninger nødvendige for at gennemføre kontaktaktiviteterne. Ønskes det at ringe via en eksisterende telefon som findes på arbejdsstationen – f.eks. en SIP-telefon eller fastnettelefon installeret af virksomheden – kan denne også bruges sammen med Hero Outbound, idet applikation kan forbinde til en ekstern telefon og holde linjen åben, hvormed der forbindes og tales via den eksterne telefon.

Et centralt system blandt andre forretningssystemer

På integrationssiden tilbyder Hero Outbound en række muligheder for at integrere med andre løsninger for så vidt angår data ind og ud af platformen; brugeroprettelse; dokumentation af telefonopkald o.m.a. Hero Outbound har et veludbygget API, som kunder kan benytte uden meromkostning. Dette REST-API tillader adgang til kundens Hero Outbound-data ud fra rettigheder på funktions- og projektniveau, som defineres af kunden selv, og muliggør at hente, opdatere og slette logiske entiteter. Hvis kunden i højere grad ønsker data push'et fra Hero Outbound til eksterne systemer, i stedet for at pull'e data fra vores REST-API, har platformen indbyggede "triggers" – en slags webhooks – hvor regler kan opsættes til at udføre bestemte handlinger når bestemte ting er forekommende i systemet. Handlinger omfatter blandt andet kald til eksterne SOAP- eller REST-API'er, hvormed man kan integrere Hero Outbound med alle andre systemer uden at skrive en eneste linje kode – så længe man har et API, som kan kaldes fra Heros webservere (et afgrænset IP-range) med enten XML eller JSON-objekter.

Ovenstående er en overordnet beskrivelse af Hero Outbound og en kort beskrivelse af nogle af de værktøjer, platformen stiller til rådighed. HeroBase ønsker med kunderne på Hero Outbound en langvarig kunderelation, hvor kunden over tid sammen med sin customer experience manager får taget større og større dele af platformen i brug, og hvor Hero Outbound integreres til andre nøglesystemer i kundens forretning. Dette tror vi muliggør sig gennem en teknisk stærk og stabil platform, hvor sikkerhed og performance er i højsædet, med et engageret teknisk og kundefokuseret team omkring sig.

Teknisk opbygning og placering

Hero Outbound er en webapplikation baseret på .NET (primært sprog er C#), med frontend baseret på bl.a. Java-script, Angular og REACT. Databaseteknologi er MySQL, og hosting sker i de danske datacentre Global Connect (Taastrup) og InterXion (Ballerup). I skrivende stund er større dele af AWS' (Amazon Web Services) løsninger ved at blive taget i brug. I første omgang med opbevaring af filer i S3 i stedet for på virtuelle servere i Danmark. Senere også med henblik på at have databaser i AWS' Aurora. De eneste AWS-lokationer, vi har valgt services i og som data dermed forefindes i, er AWS' Dublin-site i Irland samt AWS' site i Frankfurt, og der er således intet data i Hero Outbound, som forlader EU. På telefoni-siden er ringning drevet af fysiske Linux-servere med Freeswitch som teleoperativsystem ovenpå. Vores infrastruktur og arkitektur er designet således at der findes redundant failoverudstyr til alt fra firewalls og switche til database- og teleservere. Det meste udstyr forefindes også i begge datacentre, således at en lokation kan tage over, hvis en anden lokation lider under nedsat fremkommelighed eller andre problematiske forhold, interne såvel som eksterne.

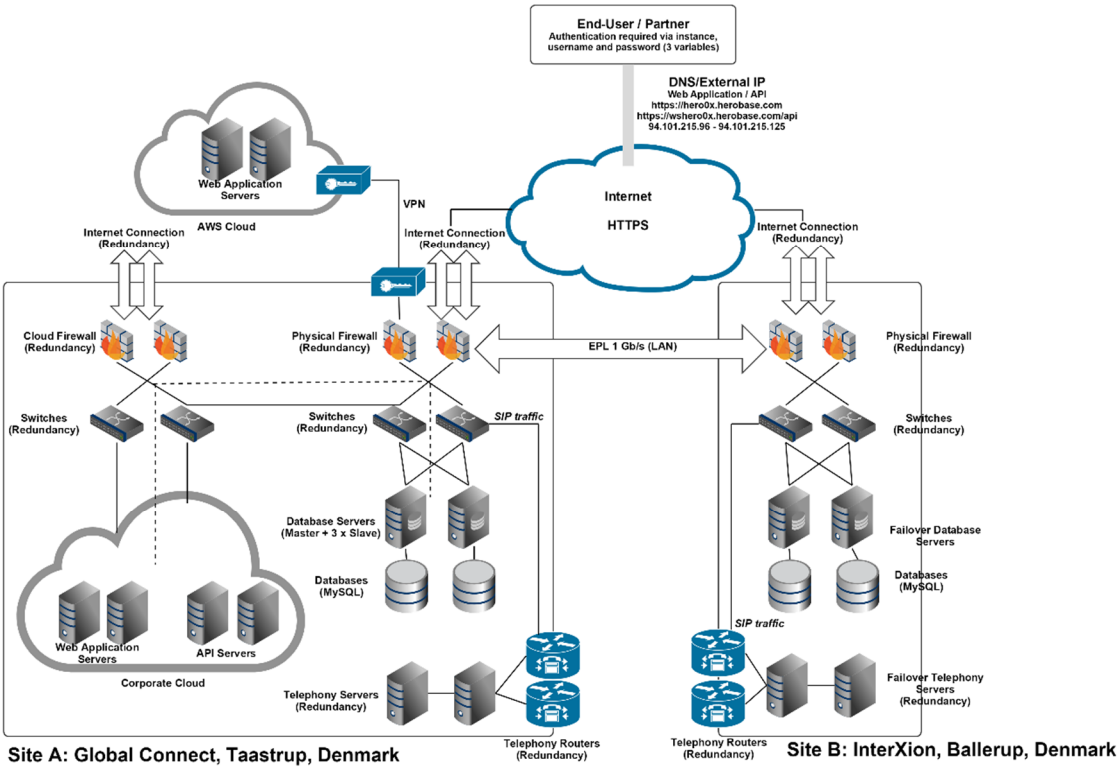

Fig. 1: Hero Outbound platformen, overordnet infrastruktur pr. medio 2018.

Vi tror på at appellere til hverdagens helte ved at designe komplette løsninger til deres arbejdspladser, og levere løsninger som gør kontaktcentre til konkurrencedygtige og effektive virksomheder ved at optimere arbejdstiden og rentabiliteten på centrenes opgaver, samtidig med at vi tilpasser platformen til nye eksterne krav såsom nye krav til betalingsløsninger, aftaledokumentation, GDPR o. lign. Vi tror på, at vi har Nordeuropas bedste software til branchen, og har internationale vækstmål baseret på et sundt og solidt hjemmemarked, hvor den gode daglige kontakt og langvarige kunderelation er i fokus!

Organisation og ansvar

HeroBase beskæftiger 30 medarbejdere i Danmark, Sverige, Ukraine, Spanien og Litauen. Godt halvdelen af medarbejderne er placeret i Danmark, og har daglig arbejdsplads på kontoret i Søborg.

Ledelsen består af en øverstansvarlig CEO, og under ham en CTO med al teknisk ansvar samt en CXO med ansvar for kundekontakt, kunderelationer og support. Hertil en stabsfunktion med CFO samt administration og HR.

IT-afdelingen, som ledes af HeroBases CTO, består primært af udviklere i en ”devops”-konstellation, hvor to mand er dedikeret til drift, optimering af servere og infrastruktur, overvågning og håndtering af operationelle issues, men hvor alle har drift som førsteprioritet i tilfælde af tekniske problemer på platformen. Det er en målsætning at egentlig udvikling, forstået som forbedring af eksisterende features og udvikling af nye, udgør 80% af afdelingens tid. Udviklerne er organiseret i frontend- og backend-ekspertiser, med en chefarkitekt som tager de overordnede beslutninger om sprog, teknologi og nye frameworks efter grundig analyse og i samarbejde med HeroBases CTO. Herudover er en netværksadministrator ansvarlig for netværk og telefoni, mens en projektleder og tester har et tæt samarbejde med HeroBases øvrige afdelinger.

Ledelsen er overordnet ansvarlig for IT-sikkerhed, og for at virksomhedens overordnede IT-sikkerhedspolitik overholdes.

Ved siden af den daglige funktionsopdelte organisation er der organiseret en sikkerhedsorganisation, med et informationssikkerhedsudvalg bestående af nøglemedarbejdere fra forskellige dele af HeroBase inkl. ledelsen, samt en informationssikkerhedskoordinator som har det daglige, operationelle ansvar for en række opgaver defineret i HeroBases informationssikkerhedsregelsæt. Informationssikkerhedskoordinatoren er desuden ansvarlig for at alle medarbejdere kender til informationssikkerhedshåndbogen, herunder regler og procedurer, hjælper dem med at tilgå og forstå den samt udleve og overholde reglerne. Slutteligt er ansvar for en række forhold omhandlende de forretningssystemer, som understøtter det daglige arbejde med at levere produktet og ydelsen Hero Outbound, uddelt til systemejerne.

Risikostyring i HeroBase A/S

Risikostyring i HeroBase A/S udføres inden for alle de områder, som har med leverancen af produktet og ydelsen Hero Outbound at gøre, og som dermed kan have en økonomisk konsekvens for vores kunder. Risikoanalyse, -vurdering og -styring er baseret på ISO27005, og tager udgangspunkt i konsekvensanalyser og sårbarhedsanalyser på serviceniveau. Service forstås som forretningssystemer som understøtter leverancen af Hero Outbound, samt selve Hero Outbound som kundesystem.

Forretningen i HeroBase svarer på konsekvensanalysens spørgsmål, mens IT-afdelingen i HeroBase gennemfører sårbarhedsanalyser. Sårbarhedsanalyser afrapporteres på serviceniveau, men tager udgangspunkt i aktiver, som er de fysiske og virtuelle delementer, som tilsammen udgør platformene eller forretningssystemerne. Eksempelvis er til servicen Hero Outbound en række afhængende aktiver som firewalls; switche; teleroutere; webapplikationsservere; databaseservere; telefoniservere m.v. Når afrapportering sker på serviceniveau, er det også klart at det er "laveste fællesnævner" som definerer f.eks. maksimalt mulige nedetid. Hvis en databaseserver altid vil kunne overtages af en failover-makker efter boot og DNS-skifte på 5 minutter, men det i yderste teori kan tage 15 minutter før en fysisk firewall vil være udskiftet med en bootet og konfigurationsindlæst redundant makker, er det klart at det er de 15 minutter, som vil definere den mulige nedetid.

Risikoanalyser gennemføres som konsekvens- og sårbarhedsanalyser mindst årligt, hvorefter det samlede sikkerhedsbillede bringes op for informationssikkerhedsudvalget og slutteligt HeroBases ledelse, til definition af nærmere handlinger.

Generelt om vores kontrolmål, herunder regler og procedurer, og implementerede kontroller

Det væsentligste i leverancen af produktet og ydelsen Hero Outbound er en stabil og sikker platform. Det er et erklæret og ledelsesforankret løfte at vi hellere vil bruge dobbelt så lang tid på at løse en udviklingsopgave eller anden teknisk opgave, end den kunne være løst på, for at sikre sikkerhed og stabilitet, når vi frigiver opdateringer til vores kunder.

For at leverancekæden kan fungere, og HeroBase samtidig kan fungere som konkurrencedygtig forretning herunder at opnå skalerbarhed over tid, er arbejdsgange og processer forbundet med levering af produktet og ydelsen Hero Outbound bygget op omkring vores informationssikkerhedsregelsæt, på toppen af hvilket der er defineret procedurer og kontroller med tilhørende beredskabsplaner m.m.

Aller øverst står vores top level information security policy, som er underskrevet af HeroBases CEO og sætter rammerne for arbejdet med informationssikkerhed. Denne gælder alle medarbejdere og nærtstående samarbejdspartnere (f.eks. konsulenter).

Referencerammen for informationssikkerhedsregelsættet er ISO27001, og regelsættet er derfor overordnet inddelt i følgende kontrolområder:

- Styring af informationssikkerhed og sikkerhedspolitik
- Organisering af informationssikkerhed
- Personalesikkerhed
- Styring af aktiver
- Adgangsstyring
- Kryptografi
- Fysisk sikring og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold
- Styring af informationssikkerhedsbrud og -hændelser
- Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
- Overensstemmelse

Vi har desuden tilvalgt en række procedurer og politikker inden for rammerne af datasikkerhed og GDPR, og tager vores ansvar som databehandler for nogle af landets største virksomheder ekstremt seriøst. Op til effektueringen af GDPR har vi udvidet vores platform med en række features, som gør det nemmere for vores kunder som dataansvarlige at leve op til de krav, de bliver stillet af bl.a. GDPR. Vi vil gerne anses som data*med*ansvarlige i højere grad end som databehandler, og udtaler os gerne om dette i forskellige sammenhænge. Som databehandler har vi desuden sikret at vi har en databehandleraftale med alle vores kunder på Hero Outbound, som i denne konstellation er dataansvarlige.

GDPR og HeroBases rolle og ansvar som databehandler

GDPR er for alle – men det er essentielt at forstå, hvordan de specifikke dele af GDPR finder anvendelse for hver enkelt aktør afhængig af hvilken type organisation, der er tale om, og hvordan organisationen er genstand for aktiviteter knyttet til behandling af persondata.

HeroBase er naturligvis dataansvarlig for vores egne data. Det betyder at vi har gennemført dataflowanalyser inden for samtlige processer i vores forretning, hvor persondata opbevares eller udveksles (internt eller med tredjepart). Dataflowanalyserne gør os i stand til at se, præcis hvilke datatyper for hvilke typer datasubjekter, som flyttes eller opbevares, samt med hvilken hjemmel.

Herudover er HeroBase som udbyder af softwaren og løsningen Hero Outbound, databehandler for alle vores kunder. Dette betyder at vi i vores software Hero Outbound hoster data, som tilhører vores kunder som dataansvarlige, og at vi gennem vores software stiller en række værktøjer og funktioner til rådighed, med hvilke vores kunder – de dataansvarlige – kan arbejde med data. Vi handler alene ud fra instruks fra vores kunder, og rammerne for disse instrukser er defineret gennem kontrakten mellem kunden og HeroBase, samt den tilhørende databehandleraftale.

Artiklerne 4-49 i GDPR finder således overordnet anvendelse hos HeroBase. Men særligt relevant i relation til HeroBases rolle som databehandler er, at vi er særligt opmærksomme på distinktionen mellem egne data og vores kunders data. Data (og services – systemer – hvori data forefindes) er klassificeret og mærket herefter, og alle tekniske og organisatoriske foranstaltninger – herunder interne procedurer og træning – og bygget op efter denne skelnen.

De følgende kapitler gennemgår disse forhold og aspekter mere specifikt, med fokus på HeroBases rolle som databehandler, dvs. forhold som vedrører vores behandling af de dataansvarliges data, og hvordan vores software Hero Outbound er designet til at understøtte vores kunder som dataansvarlige i de krav, GDPR stiller til dataansvarlige.

Principper for behandling af personoplysninger

Hero Outbound er en generisk og fleksibel platform, som muliggør indlæsning og indtastning af i princippet hvilke som helst data. Kampagneskabeloner, felter (med tilhørende attributter såsom datatype, feltvalidering m.m.) defineres, oprettes og vedligeholdes af kunden selv, som suverænt bestemmer og er ansvarlig for hvilke data, som indlæses til, opbevares i, behandles i, udlæses af og slettes fra Hero Outbound.

HeroBase som leverandør hverken tilgår eller bearbejder disse data, med mindre vi modtager en eksplicit instruks fra den dataansvarlige kunde om at bistå med f.eks. indlæsning af data eller berigtigelse/ændring af data i forbindelse med kundens kampagneaktiviteter.

Der findes en databehandleraftale mellem HeroBase og alle kunder. Indhold og principper for denne præciseres i senere afsnit.

HeroBase har gennem procedurer og kontinuerlig træning sikret, at klassifikationen af kundedata og de dertilhørende behandlingsprincipper er kendte af alle medarbejdere.

Lovlig behandling

Hvis HeroBase modtager instrukser fra kunden, som det vurderes er i strid med gældende lovgivning eller i øvrigt sunde principper for databehandling, gør HeroBase uden unødigt ophold kunden opmærksom på dette.

HeroBase udveksler eller videregiver i ingen tilfælde kundens data med tredjepart. Undtaget herfor er situationer, hvor national særlovgivning kræver at HeroBase udleverer information, f.eks. hvis danske myndigheder forespørger på data på bestemte telefonopkald som led i en efterforskning. I sådanne tilfælde vil den eneste personhenførbare data, som udleveres, være et telefonnummer – ingen øvrig persondata.

HeroBase har herudover som en del af vores informationssikkerhedsregelsæt og informationssikkerhedsprocedurer, defineret ansvar for kontakt med relevante myndigheder, hvor dette er påkrævet.

Vi har defineret kontroller for, at kundedata ikke tilgås af medarbejdere i andre sammenhænge end for at bistå kunden med support, eller hvis særskilte instrukser er modtaget fra kunden.

Samtykke

Hero Outbound muliggør gennem tidligere omtalte kundeoprettede kampagneskabeloner og feltdefinitioner, at kunden opretter felter i Hero Outbound til eksplicit dokumentation af samtykke og tilladelser givet af personer, som er genstand for salgs-, telemarketing- og kommunikationsaktiviteter gennem Hero Outbound – disse personer benævnes også som ”emner”.

Nærmere specifikt kan der oprettes felter til f.eks. ”URL til konkurrence eller hjemmeside hvor emne har givet sit samtykke”, ”type af samtykke eller tilsagn givet”, ”dato og tidspunkt for samtykke”, ”IP-adresse (hvis forefindes) hvorfra samtykke er givet” og lignende.

Ovenstående eksempler vil typisk være data, som forefindes og med fordel kan indlæses på emnet *inden* behandling gennem Hero Outbound.

I mange tilfælde vil dialogen, som emnet er genstand for, kunne afføde behov for at yderligere samtykke, tilladelse eller accept (f.eks. af en ordre) registreres. I disse tilfælde kan tilsvarende felter oprettes i Hero Outbound, eksempelvis kanalafhængig tilladelse til kommunikation og markedsføring, fortsat interesse i modtagelse af digital kommunikation, udfald på præsentation af salgstilbud og lignende.

Disse samtykker, tilladelser og accepter kan opsamles gennem dataindtastning i felter, ved at udsende et link til digital accept hvis svar opdateres ind i Hero Outbound via softwarens tilhørende REST-API, eller gennem optagelse af mundtlig accept.

Behandling af forskellige kategorier af personoplysninger

Vi har klassificeret alle data tilhørende vores kunder som dataansvarlige, som "kundedata". Disse er underlagt højeste sikkerhedsklassifikation, og vi har således ikke lavere sikkerhedsklassifikation på artikel 6 data, end vi har på artikel 9 eller -10 data.

Vi har en databehandleraftale med alle vores kunder. Når denne er baseret på HeroBases databehandleraftaleskabelon, har vi bedt kunden redegøre for hvilke typer af persondata (kategoriseret efter artikel 6, 9, 10 hhv. 87), kunden agter at indlæse og indtaste i Hero Outbound.

Vi opgør to gange om årligt om der er en stigende tendens til tilkendegivelse af indlæsning/indsamling af artikel 10 data, og såfremt det er tilfældet, laver vi en designanalyse af hvorvidt dele af vores software bør afgrænses på kategoriniveau til særligt at tage højde for særligt følsomme data, eksempelvis ved at lade kundeadministratorer definere på feltniveau i kampagneskabeloner, hvorvidt et felt med største sandsynlighed vil indeholde artikel 6, 9, 10 eller 87 data. Vi har dog i skrivende stund ikke vurderet, at dette behov er til stede endnu.

Vi er opmærksomme på at artikel 87 ikke er en egentlig datakategoriartikel på linje med 6, 9 eller 10, men særbestemmelsen om nationalt identifikationsnummer. Vi har dog alligevel valgt at benævne CPR-nummer "artikel 87-data" af forståelsesmæssige årsager.

Vi har anerkendt at det er naturligt for en række af vores kunder at artikel 9-data forefindes i Hero Outbound, idet vi har en relativt stærk repræsentation inden for forsikrings-, arbejdsløshedskasse- og fagforeningsbrancherne.

Den registreredes rettigheder

Hero Outbound registrerer alle ændringer på data på et emne, der behandles i vores software, samt alle interaktioner med det pågældende emne.

Vores kunder kan som dataansvarlige fremsøge alle emner indlæst og behandlet i Hero Outbound, og se en fuld liste over interaktioner med hvert enkelt emne.

Vores kunder kan som dataansvarlige fremsøge alle emner indlæst og behandlet i Hero Outbound, og se en fuld liste over al data, der findes på de enkelte emner.

Vores kunder kan som dataansvarlige fremsøge alle emner indlæst og behandlet i Hero Outbound, og se en fuld liste over ændringer, der har fundet sted i data på det enkelte emne.

Således registreres alle behandlingsaktiviteter eksplicit, og er tilgængelige for kunden direkte i Hero Outbounds brugergrænseflade.

Vores kunder kan som dataansvarlige fremsøge enkelte emner, blokere dem for fremtidig kontakt, og/eller slette al data, der findes på de enkelte emner.

Vores kunder kan som dataansvarlige fremsøge enkelte emner, og redigere/berigtige information på de enkelte emner.

Vores kunder kan som dataansvarlige eksportere ovennævnte data, således at data kan fremsendes til et datasubjekt; slettes fra Hero Outbound; og datasubjektet med sine data kan flyttes til et andet system eller serviceydelse.

Hero Outbound understøtter således vores kunder som dataansvarlige i at overholde de registreredes rettigheder, og i udgangspunktet håndtere disse effektivt og uden unødigt ophold.

Generelle forpligtelser som databehandler

Vi har procedurer, som sikrer at vi overholder vores forpligtigelser som databehandler, og i videst mulig udstrækning understøtter og supporterer vores kunder som dataansvarlige i forhold til de krav, GDPR stiller til dem.

Vores funktioner til understøttelse af de registreredes rettigheder, jf. foregående afsnit, er samlet på få forskellige sider i Hero Outbound, som gennem modul- og rettighedsstyring hos kunden selv sikrer vores kunder mulighed for at tildele funktionsrettigheder til at betjene funktionerne, efter arbejdsbetinget behov hos kunden.

Skulle HeroBase modtage en henvendelse fra et datasubjekt direkte, uden om kunden, vil HeroBase inden for lovgivningens rammer anmode datasubjektet om yderligere information, og uden unødigt ophør sende henvendelsen eller anmodningen videre til vores kunde. Vi har procedurer for dette, som er kommunikeret til og trænet hos vores medarbejdere.

Vi har sikret databehandleraftaler med underdatabehandlere, herunder hosting- og housing-partnere.

Vi har sikret at de krav, der stilles fra vores kunder til os gennem kontrakten og databehandleraftalen, er tilsvarende stillet og forankret hos underleverandører og underdatabehandlere.

Vi sikrer gennem løbende uddannelse og kampagner en bevidsthed om væsentlige områder inden for informationssikkerhed, databeskyttelse samt (men ikke afgrænset til) GDPR.

Vi har procedurer for, at databeskyttelse indgår i designovervejelser og -valg, når Hero Outbound ændres og videreudvikles.

At handle ud fra instruks fra vores dataansvarlige kunder omfatter også hvor længe data opbevares i Hero Outbound. Data forstås her som både skrevne data (talværdier, tekststrenge og øvrige indtastninger – det, som i klassisk forstand forstås som data) og multimediedata (lydfiler fra samtaler, vores kunder måtte have valgt at optage gennem Hero Outbound).

Instrukserne gives til HeroBase som databehandler gennem indstillinger, kunden sætter op i Hero Outbound.

Alle emner tilhører kampagner, som tilhører projekter. På projektniveau kan sletteregler for data defineres, således at alle (eller udvalgte) data på emner afsluttet med bestemte statusser automatisk slettes efter ”x” dage.

Disse regler eksekveres natligt på Hero Outbounds databaseservere, og sletter data ud fra regler opsat af vores kunder.

Data opbevares på en backup i 7 dage, hvorefter data også slettes fra backup, og dermed efter 7 dage vil være fjernet fra alle databaseinstanser uden mulighed for genskabelse

Behandlingssikkerhed, anmeldelse og underretning

Vi har passende tekniske og organisatoriske foranstaltninger på plads, hvilket uddybes i senere hovedafsnit.

ISO27001 er valgt som informationssikkerhedsrammen, som vores informationssikkerhedsregelsæt, procedurer og kontroller er baseret på.

Vi har procedurer for håndtering af informationssikkerhedsbrud, herunder datalæk, samt informationssikkerhedshændelser.

Vi har procedurer for indberetning til relevante myndigheder i tilfælde, hvor det er nødvendigt, samt underretning af vores kunder som dataansvarlige, såfremt brud eller hændelser vedrører disse eller kan komme til at gøre det. Dette gøres inden for tidsfrister, som er defineret i databehandleraftalerne.

Konsekvensanalyse

Vi har procedurer for udførsel af konsekvensanalyser/DPIA, i forbindelse med gennemførsel af projekter og udvikling af Hero Outbound som software.

Databeskyttelsesrådgiver (DPO)

HeroBase har fravalgt at have en databeskyttelsesrådgiver (DPO), jf. artikel 37. Årsagen til fravalget er at HeroBase råder over en relativt beskeden mængde persondata, hvor HeroBase selv er dataansvarlig, og således har fremmeste rolle som databehandler og udbyder af Hero Outbound. På denne baggrund behandler HeroBase ikke persondata systematisk, ligesom der ikke er tale om store mængder af følsomme eller særligt følsomme oplysninger.

Vi har i stedet udpeget og organiseret en komplet sikkerhedsorganisation ved siden af den almindelige driftsorganisation. Sikkerhedsorganisationen består af et informationssikkerhedsudvalg samt en informationssikkerhedskoordinator. Udvalget og koordinatoren sikrer forankring af det løbende arbejde med informationssikkerhed, og har desuden en række forpligtelser defineret af vores informationssikkerhedsregelsæt og procedurer.

Overførsel af personoplysninger

Al data i Hero Outbound tilhører vores kunder, og HeroBase videregiver, overdrager eller udveksler i ingen sammenhænge data med tredjepart. Al udveksling, udlæsning og overførsel af data sker kun af kunden selv ved at benytte funktioner i Hero Outbound eller vores tilhørende REST-API.

Vores hosting- og housing-partnere, som vi har underdatabehandleraftaler med, har kun data opbevaret i EU, jf. tidligere afsnit. Data i Hero Outbound overføres således aldrig til tredjelande, med mindre kunden uden om HeroBase vælger selv at gøre det.

Vi har desuden procedurer som omhandler portabilitet af data, herunder håndtering af fysiske medier.

Tekniske og organisatoriske foranstaltninger

Vi ønsker i dette afsnit at uddybe en række forhold vedr. HeroBases tekniske og organisatoriske foranstaltninger, som gælder levering og drift af softwaren og ydelsen Hero Outbound.

Personalesikkerhed

Vi har defineret en række procedurer som sikrer sikkerhed før, under og evt. efter ansættelsen.

Procedurer som omhandler processer før en evt. ansættelse sikrer, at potentielle medarbejdere screenes og at relevante forhold kontrolleres inden for rammerne af gældende lovgivning.

Alle medarbejdere skal leve op til en række vilkår om fortrolighed om egne, HeroBases og kunders forhold. Dette er beskrevet i ansættelseskontrakten for hver medarbejder.

Under ansættelsen sikres det sammen med medarbejderen, nærmeste leder og informationssikkerhedskoordinatoren, at medarbejderen holdes ajour indenfor og efterleverer aspekter vedrørende informationssikkerhed.

Vi har procedurer som sikrer at medarbejdere ved ansættelses ophør ikke kan forvolde HeroBase eller systemet Hero Outbound skade, ved øjeblikkeligt at fjerne rettigheder til forretningssystemer og kontrollere dette.

Der er desuden defineret en række sanktioner såfremt informationssikkerheden overtrædes eller tilsidesættes.

Styring af aktiver

Alle aktiver er defineret med ejerskab, kritikalitet og tekniske afhængigheder som services, der afhænger af enkelte aktiver. Servere, systemer, netværk mv. er dokumenteret og til rådighed for relevant teknisk personale. Ved introduktion af nyt udstyr og nye systemer, eller ved ændringer i arkitekturen og infrastrukturen, opdateres relevant dokumentation således at denne altid er ajourført.

Der er defineret acceptabel brug af systemer for medarbejderne, hvilket bl.a. indebærer retningslinjer for at tilgå, bruge og eksportere data. Data anskues kategoriseret efter GDPR's kategorier hertil, og særlige procedurer gælder for visse datatyper.

Vi har procedurer som omhandler styring af bærbare medier, bortskaffelse af medier samt transport af bærbare, databærende medier, samt for klassifikation og mærkning af data. Dette betyder blandt andet (men er ikke afgrænset til) at data udelukkende må forefindes i systemer og på fysiske og virtuelle servere mærket og angivet til formålet. Kundedata må som udgangspunkt ikke forefindes andre steder, herunder lokalt, på USB-nøgler, på andre diske (flash drives) o. lign. En undtagelse herfor er hvis en kunde skriftligt har anmodet om at få udleveret data, eller hvis det er nødvendigt at flytte data mellem to servere, og transporten ikke kan ske via netværk.

Lagres data midlertidigt på sådanne USB-nøgler, drev o. lign., skal data i videst mulig udstrækning anonymiseres eller pseudonymiseres, og den fysiske enhed (herunder mapper på den) skal beskyttes af password. Disse medier må som udgangspunkt aldrig postforsendes til kunder, men skal transporteres af HeroBases medarbejdere, eller afhentes af kunden.

Når fysiske servere tages ud af drift, og data på harddiske ikke længere har behov for at forefindes på pgl. diske, skal diskene enten a) formateres således at genskabelse af data ikke længere er mulig, b) fysisk ødelægges og diskene bortskaffes af medarbejdere i HeroBases IT-afdeling, eller c) begge dele.

Adgangsstyring

Vi har en række procedurer som sikrer at adgangskontrol og rettighedstildeling sker i overensstemmelse med det fastlagte sikkerhedsniveau.

Kun medarbejdere, som har et arbejdsrelateret behov for at have adgang til systemer og data, får adgang til pågældende forretningssystemer med tilhørende data.

Afdelingslederne er ansvarlige for at adgangsrettigheder tildeles ud fra et arbejdsbetinget behov samt under hensyntagen til lovgivningsmæssige og kontraktlige forpligtigelser.

Vi har en række kontroller som kontrollerer at dette sker løbende, og at alle adgange modsvarer de arbejdsrelaterede behov i de enkelte funktioner og hos de enkelte medarbejdere.

Vi har defineret en række krav til alle enheders beskyttelse (PC'er, mobiltelefoner, tablets) samt passwords i alle forretningssystemer. Medarbejdere uddannes og kontrolleres løbende inden for disse områder.

Vi har en række procedurer som sikrer at kun en lille gruppe privilegeret personale har adgang til systemadministratorværktøjer, centrale servere (f.eks. domain controller), kildekode mv.

Produktionsservere og øvrige servere med produktionsdata og kundedata forefindes kun i HeroBases datacentre, og ikke på nogle kontorlokationer. Kun særligt betroede medarbejdere med et arbejdsrelateret behov har adgang hertil. Disse adgange revalueres og efterses løbende.

Kryptografi

Vi har procedurer for anvendelse af kryptografi, herunder generering og håndtering af krypteringsnøgler og certifikater.

Dette betyder bl.a. at Hero Outbound skal have et gyldigt SSL-certifikat, HeroBase selv kontrollerer, således at dataudveksling kun sker sikkert og krypteret (gennem HTTPS). SSL-certifikater styres udelukkende af IT-afdelingen, hvor applikationsarkitekten og netværksadministratoren har ansvaret for SSL-certifikater. Ingen certifikater må købes eller udstedes uden om disse.

Dette krav omfatter både adgang til Hero Outbound gennem brugergrænsefladen og gennem API.

Fysisk sikring og miljøsikring

Servere forefindes kun i datacentre udbudt af leverandører som har fået afgivet, og årligt kan fremvise, erklæringer på niveau med ISAE3402.

HeroBases kontorlokation er underlagt en række procedurer som sikrer kontoret samt materiale og enheder opbevaret på kontoret, upåagtet at servere kun forefindes i datacentre.

Dette betyder bl.a. procedurer rettet mod medarbejderne, der beskriver sikringstiltag for kontorer, fællesområder og lign. områder.

Driftssikkerhed

Driftsprocedurer og overvågning

Vi har driftsprocedurer for IT-afdelingens væsentligste arbejdsopgaver, og disse procedurer er omfattet af versionering og ændringsstyring.

Vi har defineret ansvar for at sikre, at der løbende bliver foretaget en vurdering af kapacitetsbehovet for kritiske it-systemer.

Pga. vores størrelse kan vi ikke have fuldstændigt overlap på samtlige funktioner, men jf. tidligere beskrivelse tilstræber vi qua funktionsadskillelse og grundig og løbende dokumentation og vidensdeling at undgå personafhængighed. IT-afdelingen, som ledes af HeroBases CTO, består primært af udviklere i en "devops"-konstellation, hvor to mand er dedikeret til drift, optimering af servere og infrastruktur, overvågning og håndtering af operationelle issues, men hvor alle har drift som førsteprioritet i tilfælde af tekniske problemer på platformen eller informationssikkerhedsissues.

Alle instanser af Hero Outbound overvåges via monitoreringsværktøjer. Hermed overvåges blandt meget andet serveres fremkommelighed, CPU/memory/disk I&O forbrug, tilsvarende for databaseservere, lag (i milisekunder) mellem master- og slavedatabaser, tunge SQL queries foretaget af applikation eller direkte af en klient, o.m.a.

Der er for alle disse overvågningsområder defineret kritiske niveauer og værdier. Alarmer skal trigges når disse værdier nås, og sendes til nøglemedarbejdere på enten e-mail (for mindre kritiske opmærksomheder) og SMS (kritiske opmærksomheder).

Historiske logs og hændelser gennemgås løbende og struktureret med henblik på forbedringer og optimeringer.

Vi har procedurer for backups foruden løbende datareplikering, og backups brugbarhed til restore efterprøves løbende ved kontroller.

Udvikling af Hero Outbound, styring og kvalitetssikring

Udvikling af Hero Outbound, herunder release af ændringer, foregår efter HeroBases formaliserede og forankrede udviklingsmodel.

Udvikling finder sted i udviklingsmiljøer hvor kode branches ud fra hovedbranch/"default". Disse udviklingsbranches er forbundet til staging databasen hvor testdata forefindes. Testdata og produktionsdata er således komplet adskilt, og kunders data må ikke kopieres fra master til staging uden godkendelse fra HeroBases CTO. Hvis denne tilladelse gives kan og vil det kun omfatte konfigurationsdata med henblik på at teste og udvikle op imod retvisende kompleks data for at sikre kvalitet af udvikling, men det må og kan aldrig omfatte data på kundens emner, medarbejdere eller andet som er personhenførbart og kategoriserbart i henhold til GDPR's artikler 6, 9, 10 og 87.

Der funktionstestes i udviklingsbranches (også benævnt feature branches), hvorefter kode merges til preproduktion, videre til CX branch, videre til pre-release branch, videre til release branch hvorfra kode endegyldigt deployes til produktion.

Integrationstest med dertilhørende regressionstests og happy flow testing finder sted fra CX branch, prerelease branch og/eller release branch, hvor der testes på master databasen men på egne testdata. Kunders personhenførbare data indgår således ikke i tests og tilgås eller ses ikke af HeroBases medarbejdere i nogle af disse testfaser. Data i master databasen på egne konti er produceret så det strukturelt ligner produktionsdata, kunder arbejder med, hvormed datasikkerhed, fortrolighedsbehandling og samtidig kvalitetssikring sikres og balanceres.

Logning

Vi har procedurer som omhandler omfanget, behandling, beskyttelse og kontrol af logning på forskellige systemtyper.

Alle logins og væsentlige brugerhandlinger i Hero Outbound overvåges og logges. Logningen af væsentlige brugerhandlinger omhandler bl.a. dataeksport, således at kundeadministratorer har overblik over hvilke brugere, der tilgår og eksporterer data.

Alle ændringer på data registreres.

Alle væsentlige ændringer i konfigurationer registreres.

Disse registreringer er også tilgængelige for kundeadministratorer gennem synlige logs i brugergrænsefladen.

Logningsniveauet omfatter også medarbejdere hos HeroBase, hvormed det kontrolleres at disse ikke tilgår kundedata uden der er et arbejdsrelateret behov for det. Dette kontrolleres og efterprøves detaljeret på stikprøvebasis.

Kommunikationssikkerhed

Vi har procedurer for netværksstyring og overvågning, herunder vedligeholdelse af netværk og netværksudstyr.

Trafik på alle forbindelser og interfaces overvåges i forhold til datavolumen over perioder. Der er opsat alarmer som udløses og sendes til teknisk personale i tilfælde af anormaliteter (trafik spikes, væsentlige delays mellem master databaser og slave databaser, mv). På teleforbindelser bliver bl.a. antal provider kanaler, antal serverkanaler (Freeswitch kanaler) og antal igangværende opkald overvåget, og max-værdier for perioder logges.

Dette sikrer løbende korrekt kapacitetsstyring samt gardering mod misbrug.

Vi har desuden samarbejde med frauddetekteringsafdelinger hos alle teleoperatører, vi benytter som underleverandører, som et ekstra lag af sikkerhed i forhold til misbrug.

Informationsudveksling sker kun via sikre forbindelser. Går dette via det offentlige internet bliver data krypteret (som udgangspunkt via HTTPS). Systemer som har mulighed for at kommunikere på interne forbindelser (på intern IP-adresse bag firewall - og mellem datacentre ad fiberforbindelse hvorigennem servere på forskellige lokationer også kan nå hinanden på intern IP-adresse) benytter denne metode til dataudveksling via LAN.

Leverandørforhold

Vi har i alle samarbejdsaftaler med leverandører defineret sikkerhedskrav og minimumskrav til ydelserne, vi modtager fra leverandøren.

Vi har sikret at de forhold, vi baserer vores aftale om brug af produktet og ydelsen Hero Outbound på over for vores kunder, er overensstemmende med de krav vi stiller til vores leverandører.

Vi gennemgår løbende og mindst årligt samarbejdsaftalerne, ligesom vi indhenter revisionserklæringer for de indgåede aftaler.

Vi har defineret ansvar for kvartalsvist at gennemgå rapporter fra de eksterne serviceleverandører på operationelt udstyr, omhandlende hændelser, problemer, fejl, nedbrud og logning.

Styring af informationssikkerhedsbrud og -hændelser

Informationssikkerhedsudvalget har defineret procedurer for informationssikkerhedsbrud og -hændelser, som er forankret i HeroBase og som ledelsen har ansvaret for overholdelsen af.

Vi definerer informationssikkerhedsbrud som:

- Detektering af succesfuld udefrakommende og uønsket indtrængen i systemer
- Fund af kundedata (hostet i masterdatabase for Hero Outbound) online, hvor der er åbenlys eller kraftig mistænke om at offentliggørelse af data ikke er sket med kundens godkendelse og forsæt

- Fund af data på nuværende eller tidligere medarbejdere i HeroBase online, hvor offentliggørelse af data er sket uden HeroBases medvirkende eller forsæt
- Fund af andre fortrolige forretningsdata online (efter samme forskifter) defineret som kundekontrakter, omsætning eller informationer som er klassificeret som hemmelige efter nærmere definition af informationssikkerhedsudvalget

Vi definerer informationssikkerhedshændelser som:

- Hændelser som, hvis de ikke var blevet opdaget, kunne have ført til sikkerhedsbrud
- Situationer hvor utilsigtet data eller information ved et uheld (ved menneskelig fejl) er blevet sendt til andre modtagere end de tilsigtede, og det vurderes at dette kan medføre skade eller alvorlige konsekvenser for HeroBase

Der er defineret procedurer for begge, som beskriver for medarbejdere og ledere, hvordan de skal forholde sig ved brud og hændelser, inkl. (men ikke afgrænset til) indsamling af bevismateriale og kontakt til myndigheder, hvis nødvendigt.

Alle medarbejdere er bekendte med instrukserne og træner heri.

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Vi har defineret ansvar for udarbejdelse af nødplaner, beredskabsplaner og reetableringsplaner.

Vi har etableret tilstrækkelig redundans for at imødegå kravene til tilgængelighed og de garantier for oppetid, vi har kontrakt med vores kunder på.

Alle tekniske medarbejdere er trænet i planerne.

Planer og procedurer evalueres løbende og efter hvert operationelt issue, hvor menneskelig handling har været nødvendigt for at reetablere drift på dele af platformen.

Fuld transparens for de dataansvarlige

Vi har, ud fra en defineret vision om at vores kunder som dataansvarlige skal kunne tilegne sig så meget indsigt i alle forhold relateret til potentiel platformsbrug og -sikkerhed som muligt, uden at henvende sig til os som softwareudbyder, gjort en række yderligere oversigter og parametre synlige for kunden i Hero Outbound.

Vi viser en log over brugerhandlinger, som har ført til visning af mange emners data på skærmen på samme tid, og som kan have ført til en eksport af data. At udføre dette i Hero Outbound vil i mange sammenhænge blot være lig med at løse daglige administrative opgaver, men da handlingerne i teorien kan være første skridt i en uhensigtsmæssig brug af systemet, som ultimativt kan føre til databrud, tror vi på en præventiv effekt ved at stille disse informationer til rådighed for vores kundeadministratorer.

Vi viser en log over logins i kundens Hero Outbound-konto, med bruger, tidspunkt og ip-adresse.

Vi viser oversigter over konfigurationsændringer på kampagner, herunder opsætning af de nævnte ”triggers”, som kan sende data fra Hero til eksterne systemer.

Vi ønsker at ”privacy by design” skal være en fuldstændig indbygget del af Hero Outbounds platformdesign, og har bl.a. indarbejdet forhold affødt af GDPR i fundamentale entiteter og begreber i vores platform. Som forklaret repræsenteres alle privatpersoner/datasubjekter (samt andet, som behandles i Hero Outbound – eksempelvis virksomheder) ved ”emner”, og disse har altid en status (benævnt emnestatus eller LeadStatus), som Hero Outbound bruger til styring af næste handling for emnet samt i rapporteringsmæssige

øjemed. Når kundeadministratorer ved henvendelser fra datasubjekter sletter deres data fuldstændig ved udnyttelsen af retten til at blive glemt, og/eller placerer emnets telefonnummer på en liste for frabedt fremtidig kontakt, har emnet særlige statusser til præcis dette, for klart at skelne mellem disse og andre handlinger i behandlingen af emner. Nedenstående uddrag af dokumentationen fra Hero Outbounds REST-API eksemplificerer, hvordan disse begreber er blevet gjort til en fundamental del af platformdesignet i Hero Outbound.

```
/// <summary>
/// User request to clear info about him, all lead data is cleared from
the system according
/// </summary>
Anonymized = 610,

/// This status can be set by administrators to signal that the lead
/// should not be called, since it in corporate's DoNotCall list.
/// </summary>
DoNotCall = 700,
```

Overensstemmelse

Nærværende rapport er udarbejdet for at levere dybdegående information til vores kunder og deres interessenter (herunder revisorer) vedrørende kravene og indholdet i databeskyttelsesforordningen (”GDPR”). Som led i kontrol af implementeringen og forankringen af vores tekniske og organisatoriske foranstaltninger, er en ISAE3402-erklæring udarbejdet ved siden af denne erklæring.

Vi kontrollerer løbende at regler og procedurer bliver efterlevet, fulgt og dokumenteret.

Vi sikrer at vi handler inden for gældende lovgivning og i øvrigt efterlever krav som stilles til dokumentation af national lovgivning.

Vi sikrer at persondata beskyttes og behandles i overensstemmelse med Persondataloven og GDPR.

ISO27001 har i årevis været brugt som referenceramme for informationssikkerhed i HeroBase og omkring udvikling og drift af Hero Outbound. Den nævnte ISAE3402-erklæring er vores første ISAE3402-erklæring på leverance af produktet og ydelsen Hero Outbound, hvorfor der er tale om en type I-erklæring. Det er forankret i ledelsen at efterlevelsen af regler og procedurer i vores informationssikkerhedsregelsæt, herunder kontroller som knytter sig til regler og procedurer, skal formaliseres, dokumenteres og underlægges årlig revision af en ekstern IT-revisor, hvorfor vi også for fremtiden vil få udarbejdet ISAE3402 (type II) erklæringer.

Komplementerende kontroller

HeroBase er over for vores kunder ansvarlige for at levere de ydelser og den drift, som er beskrevet i kontrakten omhandlende Hero Outbound mellem kunden og HeroBase.

Forhold, som ikke er omfattet af kontrakten, er kundens eget ansvar.

Oprettelse af brugere, beskyttelse af brugerinformationer og sikre login-procedurer er kundens ansvar. Kunden kan ved skriftlig henvendelse til HeroBase anmode om at få etableret ip-lås på kundens Hero Outbound-konto, hvormed login kun vil være muligt fra eksplicit defineret whitelistede ip-adresser. HeroBase anbefaler vores kunder at gøre dette i den udstrækning, det er muligt for kunden, for at beskytte kundens data og aktiviteter i Hero Outbound.

For så vidt angår data uploadet til Hero Outbound af kunden, er det en væsentlig ansvarsdeling at kunden er dataansvarlig og HeroBase er databehandler. HeroBase handler således alene ud fra instruks fra kunden. Kunden giver i kontrakten eller i databehandleraftalen HeroBase tilkendegivelse af, hvilke typer/kategorier af data, kunden har intentioner om at uploade til og behandle i Hero Outbound. Der skal forefindes en databehandleraftale mellem HeroBase og kunden.

For så vidt angår GDPR stiller HeroBase en række funktioner til rådighed på platformen Hero Outbound, som gør det muligt for kunden at leve op til GDPR's krav til dataansvarlige. Disse funktioner indbefatter (men er ikke afgrænset til) mulighed for at fremsøge data samt log over alle interaktioner mellem agent og "emner", mulighed for at berigtige data, mulighed for at slette data o.m.a.

Det er kundens ansvar at have defineret og forankret en procedure hos kunden, som sikrer efterlevelse af GDPR ved bl.a. at leve op til kravene om svartider ved henvendelser fra privatpersoner/datasubjekter. HeroBase stiller funktioner til rådighed gennem værktøjet Hero Outbound, men kan ikke holdes ansvarlig for kundens definition, forankring og efterlevelse af procedurer som skal sikre kundens overholdelse.

Uafhængig revisors erklæring om overholdelse af databeskyttelsesforordningen (GDPR) pr. 17. december 2018

Til HeroBase A/S' ledelse, selskabets kunder og disses revisorer

Vi har efter aftale undersøgt HeroBase A/S' løsning Hero Outbound for overholdelse af databeskyttelsesforordningen (GDPR) pr. 17. december 2018.

Vores konklusion udtrykkes med høj grad af sikkerhed.

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

Ledelsens ansvar

Ledelsen i HeroBase A/S har ansvaret for at implementere og sikre opretholdelsen af forretningsgange som krævet af databeskyttelsesforordningen (GDPR).

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).

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 vores konklusion.

REVI-IT A/S er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender således et omfattende 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 integritet, 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 behandling 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

HeroBase A/S' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved Hero Outbound, 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

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).

Det er vores opfattelse, at HeroBase A/S' løsning Hero Outbound, i alle væsentlige henseender, lever op til ovennævnte kriterier pr. dags dato, 17-12-2018.

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 HeroBase A/S' løsning Hero Outbound, 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, 17. december 2018

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 HeroBase A/S har implementeret i henhold til overholdelse af databeskyttelsesforordningen (GDPR). 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. 17-12-2018 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 HeroBase A/S' 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 HeroBase A/S 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

2: Principper

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
5 - Principper for behandling af personoplysninger	Der efterleves procedurer og kontroller, som sikrer, at indsamling, behandling og opbevaring af personoplysninger sker i overensstemmelse med principperne for behandling af personoplysninger.	Vi har forespurgt til opdaterede og ledelsesgodkendte skriftlige procedurer for behandling af personoplysninger, der omfatter principper for behandling af personoplysninger, og vi har inspiceret procedurerne. Vi har forespurgt til løbende kontrol af overholdelse af principperne, og vi har inspiceret kontrollen.	Ingen væsentlige afvigelser konstateret.
6 - Lovlig behandling	Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.	Vi har forespurgt til opdaterede og ledelsesgodkendte skriftlige procedurer for behandling af personoplysninger, og vi har inspiceret procedurerne. Vi har forespurgt til lovlig hjemmel til at behandle personoplysninger, og vi har inspiceret hjemlen. Vi har forespurgt til løbende kontrol af, at behandling sker på et lovligt grundlag, og vi har inspiceret kontrollen.	Ingen væsentlige afvigelser konstateret.
7 - Betingelser for samtykke 8 - Betingelser for et barns samtykke i forbindelse med informationssamfundstjenester	Der efterleves procedurer og kontroller, som sikrer, at de registrerede har givet skriftligt samtykke til behandling af personoplysninger.	Vi har forespurgt til funktionalitet i systemet til indhentning, håndtering og dokumentering af samtykke, og vi har inspiceret funktionaliteten.	Vi har observeret, at virksomheden ikke er ansvarlig for indhentning af samtykke ifm. behandling af personoplysninger, men at funktioner, der understøtter indhentelse af skriftligt samtykke, er stillet til rådighed for dataansvarlig. Ingen væsentlige afvigelser konstateret.
9 - Behandling af særlige kategorier af personoplysninger 10 - Behandling af personoplysninger vedrørende straffedomme og lovovertrædelser	Der efterleves procedurer og kontroller, som sikrer, at behandling af særlige kategorier af personoplysninger alene sker under hensyntagen til fastlagte kriterier, betingelser og de fornødne garantier.	Vi har forespurgt til opdaterede og ledelsesgodkendte skriftlige procedurer for behandling af særlige kategorier af personoplysninger, og vi har inspiceret procedurerne. Vi har forespurgt til lovlig hjemmel til at behandle særlige kategorier af personoplysninger, og vi har inspiceret hjemlen. Vi har forespurgt til løbende kontrol af, at behandling sker på et lovligt grundlag, og vi har inspiceret kontrollen.	Ingen væsentlige afvigelser konstateret.

2: Principper

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
11 - Behandling, der ikke kræver identifikation	Der efterleves procedurer og kontroller, som sikrer, at opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede opretholdes, så længe identifikation er påkrævet.	*Virksomheden foretager ikke behandling, der ikke kræver identifikation, hvorfor punktet ikke er relevant.*	*Ikke relevant.*

3: Den registreredes rettigheder

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
12 - Gennemsigtig oplysning, meddelelser og nærmere regler for udøvelsen af den registreredes rettigheder	Der efterleves procedurer og kontroller, som sikrer, at oplysninger om behandlingen af personoplysninger kan udleveres i en gennemsigtig, lettilgængelig og forståelig form til den registrerede.	*Virksomheden indsamler ikke personoplysninger som dataansvarlig, hvorfor punktet ikke er relevant.*	*Ikke relevant.*
	Der efterleves procedurer og kontroller, som sikrer, at udøvelsen af den registreredes rettigheder sker rettidigt, herunder besvarelse af den registreredes anmodninger og begrundelse for eventuelt afslag.	Vi har forespurgt til procedure for, at udøvelsen af den registreredes rettigheder sker rettidigt. Vi har forespurgt til kontrol til sikring af overholdelse af virksomhedens procedure, og vi har inspiceret kontrollen.	Ingen væsentlige afvigelser konstateret.
13 - Oplysningspligt ved indsamling af personoplysninger hos den registrerede 14 - Oplysningspligt, hvis personoplysninger ikke er indsamlet hos den registrerede	Der efterleves procedurer og kontroller, som sikrer, at den registrerede har modtaget den dataansvarliges kontaktoplysninger, oplysning om formål med behandling af personoplysningerne samt oplysning om evt. overførsel af personoplysninger til modtagere, tredjelande eller internationale organisationer.	*Virksomheden agerer som databehandler, og har ikke som en del af sine ydelser at indsamle personoplysninger hos den registrerede, hvorfor punktet ikke er relevant.*	*Ikke relevant.*

3: Den registreredes rettigheder

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
	Der efterleves procedurer og kontroller, som sikrer, at den registrerede har modtaget oplysning om retten til indsigt, berigtigelse eller sletning af personoplysninger samt begrænsning af behandlingen.	*Virksomheden indsamler ikke personoplysninger som dataansvarlig, hvorfor punktet ikke er relevant.*	*Ikke relevant.*
15 - Den registreredes indsigtsret	Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til indsigt i egne registrerede personoplysninger og behandlingen heraf er overholdt.	Vi har forespurgt til procedure for håndtering af indsigtsanmodninger fra den registrerede, herunder underretning af databehandlere og modtagere af personoplysningerne, og vi har inspiceret proceduren. Vi har forespurgt til kontrol til sikring af overholdelse af virksomhedens procedure, og vi har inspiceret kontrollen.	Ingen væsentlige afvigelser konstateret.
16 - Ret til berigtigelse 19 - Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling	Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til berigtigelse af egne registrerede personoplysninger er overholdt, herunder berigtigelse hos modtagere af personoplysningerne.	Vi har forespurgt til procedure for berigtigelse af personoplysninger, herunder underretning af databehandlere og modtagere af personoplysningerne, og vi har inspiceret proceduren. Vi har forespurgt til kontrol til sikring af overholdelse af virksomhedens procedurer, og vi har inspiceret kontrollen.	Ingen væsentlige afvigelser konstateret.
17 - Ret til sletning ("retten til at blive glemt") 19 - Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling	Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til sletning af egne registrerede personoplysninger er overholdt, herunder sletning hos modtagere af personoplysningerne.	Vi har forespurgt til procedure for sletning af personoplysninger, når virksomheden modtager en anmodning fra en registreret, og at databehandlere bliver underrettet om at slette persondata, og vi har inspiceret proceduren. Vi har forespurgt til kontrol for sikring af overholdelse af virksomhedens procedurer, og vi har inspiceret kontrollen.	Ingen væsentlige afvigelser konstateret.

3: Den registreredes rettigheder

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
18 - Ret til begrænsning af behandling 19 - Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling	Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til begrænsning af behandling af egne registrerede personoplysninger, er overholdt, herunder begrænsning hos modtagere af personoplysningerne.	Vi har forespurgt til procedure for begrænsning af personoplysninger, når virksomheden modtager en anmodning fra en registreret, og at databehandlere bliver underrettet om at begrænse persondata, og vi har inspiceret proceduren. Vi har forespurgt til kontrol til sikring af overholdelse af virksomhedens procedurer, og vi har inspiceret kontrollen.	Ingen væsentlige afvigelser konstateret.
20 - Ret til dataportabilitet	Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til at overføre egne registrerede personoplysninger til en anden dataansvarlig, er overholdt.	Vi har forespurgt til procedure for dataportabilitet af personoplysninger, når virksomheden modtager en anmodning fra en registreret, og at databehandlere er forpligtet til at bistå virksomheden, og vi har inspiceret proceduren. Vi har forespurgt til kontrol til sikring af overholdelse af virksomhedens procedurer, og vi har inspiceret kontrollen.	Ingen væsentlige afvigelser konstateret.
21 - Ret til indsigelse 22 - Automatiske individuelle afgørelser, herunder profilering	*N/A – kravene er dækket af kontrolmålet i artikel 6.*	*Ikke relevant.*	*Ikke relevant.*
23 - Begrænsninger	*N/A – området er ikke relevant i forhold til kontrolmål for en erklæring.*	*Ikke relevant.*	*Ikke relevant.*

4: Dataansvarlig og databehandler

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
24 - Den dataansvarliges ansvar	Der efterleves procedurer og kontroller, som sikrer, at dataansvarliges tekniske og organisatoriske foranstaltninger til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger er godkendt af den dataansvarlige.	Vi har forespurgt til procedure, som sikrer, at virksomheden har implementeret tekniske og organisatoriske foranstaltninger til sikring af den registreredes persondata, herunder rollefordeling, password-kontrol, logning af aktivitet osv., og vi har inspiceret proceduren. Vi har forespurgt til kontrol til sikring af overholdelse af virksomhedens procedurer, og vi har inspiceret kontrollen.	Ingen væsentlige afvigelser konstateret.
25 - Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger	Der efterleves procedurer og kontroller, som sikrer, at kravene om databeskyttelse er implementeret gennem design og standardindstillinger i virksomhedens tekniske og organisatoriske sikringsforanstaltninger.	Vi har forespurgt til, om virksomheden har taget stilling til og har implementeret databeskyttelse gennem design og databeskyttelse via standardindstillinger, og at disse løbende kontrolleres, og vi har inspiceret kontroller herfor.	Ingen væsentlige afvigelser konstateret.
26 - Fælles dataansvarlige 27 - Repræsentanter for dataansvarlige og databehandlere, der ikke er etableret i Unionen	*N/A – områderne er ikke relevante i forhold til kontrolmål for en erklæring.*	*Ikke relevant.*	*Ikke relevant.*
28 - Databehandler 29 - Behandling, der udføres for den dataansvarlige eller databehandleren	Der efterleves procedurer og kontroller, som sikrer, at behandling af personoplysninger alene sker i henhold til en kontrakt eller et andet retligt bindende dokument (databehandleraftale), samt at databehandlingen alene foretages af databehandlere, som er godkendt af den dataansvarlige.	Vi har forespurgt til dokumentation for, at virksomheden har indgået databehandleraftaler med sine databehandlere, og at disse aftaler lever op til forordningens krav til databehandlere, herunder underdatabehandlere, og vi har stikprøvevis inspiceret dokumentationen. Vi har forespurgt til periodisk kontrol for, at databehandleraftalerne er opdaterede, og vi har inspiceret kontrollen.	Ingen væsentlige afvigelser konstateret.

4: Dataansvarlig og databehandler

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
30 - Fortegnelse over behandlingsaktiviteter	Der efterleves procedurer og kontroller, som sikrer, at virksomheden fører en fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af de dataansvarlige.	Vi har forespurgt til dokumentation for, at virksomheden har udarbejdet en fortegnelse over alle behandlingsaktiviteter, og vi har inspiceret fortegnelsen. Vi har forespurgt til kontrol for, at fortegnelsen løbende opdateres og evalueres, og vi har inspiceret kontrollen.	Ingen væsentlige afvigelser konstateret.
31 - Samarbejde med tilsynsmyndigheden	*N/A – området er ikke relevant i forhold til kontrolmål for en erklæring.*	*Ikke relevant.*	*Ikke relevant.*
32 - Behandlingssikkerhed	Der efterleves procedurer og kontroller, som sikrer, at der på baggrund af en evaluering af risici er truffet passende tekniske og organisatoriske sikringsforanstaltninger mod hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af, eller adgang til, personoplysninger.	Vi har forespurgt til udarbejdelsen af en ledelsesgodkendt risikoanalyse, og vi har inspiceret risikoanalysen. Vi har forespurgt til udarbejdelsen af nødvendige procedurer og tekniske foranstaltninger, herunder bl.a. ændringsstyring, sikring mod uautoriseret adgang til personoplysninger, fysisk sikkerhed mv., og vi har inspiceret procedurerne. Vi har stikprøvevis inspiceret de implementerede tekniske og organisatoriske foranstaltninger på baggrund af ovenstående procedurer. Vi har forespurgt til kontrol for periodisk gennemgang af virksomhedens risikobillede og de dertilhørende tekniske og organisatoriske foranstaltninger, og vi har inspiceret kontrollen.	Vi har observeret, at virksomhedens risikoanalyse ikke indeholder et overblik over stillingtagen til eventuelle mitigerende handlinger foretaget på baggrund af risikovurderingen. Dertil har vi observeret, at risikoanalysen ikke ekspliciterer, hvorledes risici vil have indflydelse på de registreredes rettigheder. Vi har observeret følgende i InterXions erklæring: - Den yderste fysiske perimetersikring af én af underleverandørens datacentre har ifm. igangværende bygningsarbejde ikke været forseglet, og underleverandøren har i den forbindelse ikke haft indsat ekstra foranstaltninger for at imødegå den øgede risiko. Således har generatorer og køleanlæg kunnet tilgås uden barriere. - Overvågningen på én af underleverandørens datacentre har ved inspektion vist det forkerte tidsstempel. Forholdet blev udbedret indenfor 48 timer. - Der er for nuværende ikke en klar mapning mellem virksomhedens identificerede risici, kontrolmålene og kontrolbeskrivelsen. - Der foreligger ikke dokumentation for, at virksomheden har modtaget

4: Dataansvarlig og databehandler

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
			konsulentydelser fra Information Security Committee (INFOSEC), som kontrolbeskrivelsen foreskriver. - Ifm. stikprøvegennemgang af brugerstyring, er der i 3 ud af 25 stikprøver ikke dokumenteret proces i overensstemmelse med virksomhedens procedure for samme. Ingen væsentlige afvigelser konstateret i øvrigt.
33 - Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden 34 - Underretning om brud på persondatasikkerheden til den registrerede	Der efterleves procedurer og kontroller, som sikrer, at databehandler ved brud på persondatasikkerheden kan understøtte den dataansvarliges pligt til rettidig og fyldestgørende anmeldelse til tilsynsmyndigheden, samt underretning til de registrerede, hvis personoplysninger er omfattet af bruddet.	Vi har forespurgt til virksomhedens procedure for håndtering af persondatasikkerhedsbrud, og vi har inspiceret proceduren. Vi har forespurgt til periodisk gennemgang af proceduren, og vi har inspiceret kontrollen.	Ingen væsentlige afvigelser konstateret.
35 - Konsekvensanalyse vedrørende databeskyttelse	Der efterleves procedurer og kontroller, som sikrer, at databehandler har modtaget resultatet af den dataansvarliges konsekvensanalyse vedrørende databeskyttelse, inden der foretages behandling af personoplysninger, samt at der foretages en fornyet konsekvensanalyse ved ændring i den risiko, som behandlingsaktiviteterne udgør.	Vi har forespurgt til dokumentation for ledelsens vurdering af nødvendigheden af at gennemføre egne konsekvensanalyser på hele eller dele af databehandlingen for den enkelte dataansvarlige, og vi har inspiceret vurderingen. Vi har forespurgt til kontrol for periodisk gennemgang af stillingtagen til behovet for udarbejdelse af konsekvensanalyser, og vi har inspiceret kontrollen.	Vi har observeret, at virksomheden ikke er underlagt krav til udarbejdelse af en konsekvensanalyse på hele behandlingen. Ingen væsentlige afvigelser konstateret.

4: Dataansvarlig og databehandler

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
36 - Forudgående høring	Der efterleves procedurer og kontroller, som sikrer, at databehandler har modtaget resultatet af den dataansvarliges høring hos tilsynsmyndigheden, såfremt konsekvensanalysen viser, at behandlingen af personoplysninger vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.	*Virksomheden har ikke behandlingsaktiviteter, der giver anledning til høring hos Datatilsynet, hvorfor punktet ikke er relevant.*	*Ikke relevant.*
37 - Databeskyttelsesrådgiver	Der efterleves procedurer og kontroller, som sikrer, at der - i de tilfælde, hvor det er krævet - er udpeget en databeskyttelsesrådgiver, som opfylder krav om tilstrækkelige kompetencer, og som er anmeldt til tilsynsmyndigheden.	Vi har forespurgt til dokumentation for ledelsens vurdering af nødvendigheden af at udpege en databeskyttelsesrådgiver, og vi har inspiceret vurderingen. Vi har forespurgt til periodisk kontrol for stillingtagen til nødvendigheden af at udpege en databeskyttelsesrådgiver.	Ingen væsentlige afvigelser konstateret.
38 - Databeskyttelsesrådgiverens stilling	Der efterleves procedurer og kontroller, som sikrer databeskyttelsesrådgiverens stilling, herunder at en databeskyttelsesrådgiver ikke modtager instrukser vedrørende udførelsen af dennes opgaver, samt at en databeskyttelsesrådgiver ikke udfører opgaver eller har andre pligter, som kan medføre interessekonflikt.	*Virksomheden er ikke underlagt krav om at udpege en databeskyttelsesrådgiver. Virksomheden har derfor fravalgt at udpege en databeskyttelsesrådgiver, hvorfor punktet ikke er relevant.*	*Ikke relevant.*

4: Dataansvarlig og databehandler

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
39 - Databeskyttelsesrådgiverens opgaver	Der efterleves procedurer og kontroller, som sikrer, at databeskyttelsesrådgiveren er bekendt med omfanget af sine opgaver, inddrages tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger samt rapporterer direkte til ledelsen hos den dataansvarlige eller hos databehandleren.	*Virksomheden er ikke underlagt krav om at udpege en databeskyttelsesrådgiver. Virksomheden har derfor fravalgt at udpege en databeskyttelsesrådgiver, hvorfor punktet ikke er relevant.*	*Ikke relevant.*
40 - Adfærdskodekser 41 - Kontrol af godkendte adfærdskodekser 42 - Certificering 43 - Certificeringsorganer	*N/A – områderne er ikke relevante i forhold til kontrolmål for en erklæring.*	*Ikke relevant.*	*Ikke relevant.*

5: Overførsel af personoplysninger til tredjelande eller internationale organisationer

Artikel	Kontrolmål	Gennemgang foretaget	Resultat af test
44 - Generelt princip for overførsel 45 - Overførsel baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet 46 - Overførsler omfattet af fornødne garantier 47 - Bindende virksomhedsregler 48 - Overførsel eller videregivelse uden hjemmel i EU-retten 49 - Undtagelser i særlige situationer 50 - Internationalt samarbejde om beskyttelse af personoplysninger	Der efterleves procedurer og kontroller, som sikrer, at der alene sker overførsel af personoplysninger til et tredjeland eller en international organisation, hvis Kommissionen har fastslået, at tredjelandet, et område eller en eller flere specifikke sektorer i dette tredjeland, eller den pågældende internationale organisation, har et tilstrækkeligt beskyttelsesniveau-	Vi har forespurgt til overførsel af personoplysninger til tredjelande, og vi har inspiceret dokumentation for, at virksomheden ikke overfører personoplysninger til tredjelande.	Ingen væsentlige afvigelser konstateret.