Erklæring fra uafhængig revisor

Erklæringsafgivelse i forbindelse med overholdelse af persondataloven og tilhørende bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger med senere ændringer pr. 6. marts 2018

ISAE 3000

Fonden Center for Autisme

CVR-nr.: 17 19 55 49

Marts 2018

Indholdsfortegnelse

Fonden Center for Autismes udtalelse

Denne erklæring vedrører Fonden Center for Autismes overholdelse af persondataloven og tilhørende bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger med senere ændringer.

Pr. dags dato bekræfter vi, at vi, efter vores opfattelse, pr. 6. marts 2018, i al væsentlighed har overholdt ovennævnte kriterier.

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.

Herlev, 6. marts 2018

Fonden Center for Autisme

Marianne Tankred Luckow
Centerleder

Uafhængig revisors erklæring om overholdelse af persondataloven og tilhørende bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger med senere ændringer pr. 6. marts 2018

Til Fonden Center for Autismes ledelse, fondens kunder og disses revisorer

Vi har efter aftale undersøgt Fonden Center for Autismes overholdelse af persondataloven og tilhørende bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger med senere ændringer, pr. 6. marts 2018.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Erklæringen er alene udarbejdet til brug for Fonden Center for Autismes ledelse, fondens kunder og disses revisorer til vurdering af de tilrettelagte forretningsgange, og kan ikke anvendes til andre formål.

Ledelsens ansvar

Ledelsen i Fonden Center for Autisme har ansvaret for at implementere og sikre opretholdelsen af forretningsgange som krævet i persondataloven og tilhørende bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger med senere ændringer.

Revisors ansvar

Det er vores ansvar, på grundlag af det udførte arbejde, at udtrykke en konklusion om, hvorvidt fonden overholder de krav, der er nævnt i persondataloven og tilhørende bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger med senere ændringer.

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 fondens overholdelse af de beskrevne politikker og procedurer, hvorved vores konklusion eventuelt ikke længere vil være gældende.

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 persondataloven og tilhørende bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger med senere ændringer.

Det er vores opfattelse, at Fonden Center for Autisme, i alle væsentlige henseender, lever op til ovennævnte kriterier pr. 6. marts 2018.

Beskrivelse af test af kontroller

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

København, 6. marts 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 en forståelse for effektiviteten af de kontroller, som Fonden Center for Autisme har implementeret. 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 kontrolmål har været opnået pr. 6. marts 2018.

Vi har således ikke nødvendigvis testet alle de kontroller, som Fonden Center for Autisme har implementeret i deres løsning.

Kontroller, udført hos Fonden Center for Autismes 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 Fonden Center for Autisme via følgende handlinger:

Metode	Overordnet beskrivelse
Forespørgsel	Interview, altså forespørgsel af udvalgt personale hos fonden 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

Beskrivelse og resultat af vores tests ud fra de testede kontroller fremgår af de efterfølgende skemaer. I det omfang vi har konstateret væsentlige svagheder i kontrolmiljøet eller afvigelser herfra, har vi anført dette.

Kontrol-nr.	Kontrolmål	Revisionshandlinger	Resultat
1	Den dataansvarlige skal fastsætte nærmere interne bestemmelser om sikkerhedsforanstaltninger i myndigheden til uddybning af de regler, der fremgår af denne bekendtgørelse. Bestemmelserne skal navnlig omfatte organisatoriske forhold og fysisk sikring, herunder: – Sikkerhedsorganisation – Administration af adgangskontrolordninger – Autorisationsordninger – Kontrol med autorisationer	Vi har forespurgt til interne bestemmelser for overholdelse af persondataloven og tilhørende sikkerhedsbekendtgørelse, og vi har inspiceret de interne bestemmelser.	Ingen væsentlige afvigelser konstateret.
	Der skal endvidere fastsættes instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af edb-udstyr.	Vi har forespurgt til instrukser for anvendelse af edb-udstyr, og vi har inspiceret instrukserne. Vi har forespurgt til anvendelse af personoplysninger i ind- og uddata, og vi har inspiceret instrukser for behandling af personoplysninger.	Ingen væsentlige afvigelser konstateret.
	Desuden skal der fastsættes retningslinjer for tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for myndigheden.	Vi har forespurgt til interne retningslinjer til sikring af overholdelse af fondens sikkerhedsforanstaltninger, og vi har inspiceret retningslinjerne.	Ingen væsentlige afvigelser konstateret.
	De interne bestemmelser skal gennemgås mindst én gang hvert år med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold i virksomheden.	Vi har forespurgt til gennemgang af de interne bestemmelser, og vi har inspiceret dokumentation for gennemgang af de interne bestemmelser i det indeværende år. Vi har forespurgt til kontrol for periodisk gennemgang af interne bestemmelser.	Ingen væsentlige afvigelser konstateret.
2	Den dataansvarlige skal give den fornødne instruktion til de medarbejdere, som behandler personoplysningerne. Medarbejderne skal herunder gøres bekendt med de regler, der er fastsat i medfør af § 5.	Vi har forespurgt til intern instruktion i fondens bestemmelser, og vi har stikprøvevis inspiceret dokumentation for, at de interne bestemmelser er læst af medarbejderne.	Ingen væsentlige afvigelser konstateret.

Kontrol-nr.	Kontrolmål	Revisionshandlinger	Resultat
3	Hvis behandling af personoplysninger foretages af en databehandler på den dataansvarliges vegne, skal der foreligge en skriftlig aftale, hvoraf det fremgår, at reglerne i denne bekendtgørelse ligeledes gælder for behandlingen ved databehandleren.	Vi har forespurgt til anvendelse af underdatabehandlere, og vi har inspiceret indgåede databehandleraftaler. Vi har forespurgt til indgåelse af databehandleraftaler med dataansvarlige, og vi har stikprøvevis inspiceret indgåede databehandleraftaler.	Ingen væsentlige afvigelser konstateret.
	Hvis databehandleren er etableret i en anden medlemsstat, skal det fremgå af aftalen, at de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den medlemsstat, hvor databehandleren er etableret, gælder for denne.	Vi har forespurgt til fysisk placering af persondata.	Ingen væsentlige afvigelser konstateret.
	Hvis behandling af personoplysninger finder sted på en pc-arbejdsplads uden for den dataansvarlige myndigheds lokaliteter, skal myndigheden fastsætte særlige retningslinjer herfor, således at det sikres, at bestemmelserne om sikkerhedsforanstaltninger iagttages.	Vi har forespurgt til retningslinjer for anvendelse af fjernarbejdspladser, og vi har inspiceret retningslinjerne. Vi har endvidere inspiceret udvalgte foranstaltninger til sikring af data uden for fonden.	Ingen væsentlige afvigelser konstateret.
4	På steder, hvor der foretages behandling af personoplysninger, skal der træffes forholdsregler med henblik på at forhindre uvedkommendes adgang til oplysningerne.	Vi har forespurgt til erklæring fra underleverandør af fysisk sikkerhed, og vi har inspiceret erklæringen med henblik på at efterse de fysiske adgangskontroller og styring af adgang. Vi har inspiceret de fysiske forhold hos Fonden Center for Autisme med henblik på at kontrollere den fysiske sikring.	Ingen væsentlige afvigelser konstateret.
5	I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier, skal der træffes de fornødne foranstaltninger for at sikre, at bestemmelsen iagttages.	Vi har forespurgt til retningslinjer og procedure for reparation og service af udstyr.	Ingen væsentlige afvigelser konstateret.

Kontrol-nr.	Kontrolmål	Revisionshandlinger	Resultat
6	Inddatamateriale, som ikke indgår i en manuel sag eller i et manuelt register, må kun anvendes af personer, som er beskæftiget med inddatering. Inddatamateriale, som er omfattet af bestemmelsen, skal opbevares aflåst, når det ikke anvendes. Inddatamateriale som nævnt i stk. 1 skal slettes eller tilintetgøres, når det ikke længere skal anvendes til de formål, som behandlingen varetager, eller til kontrol med de inddaterede personoplysninger, dog senest efter en af den dataansvarlige myndighed nærmere fastsat frist. Ved tilintetgørelse af inddatamateriale skal der træffes de fornødne sikkerhedsforanstaltninger mod, at materialet misbruges eller kommer til uvedkommendes kendskab.	Vi har forespurgt til behandling af persondata i inddatamateriale, og vi har inspiceret retningslinjer og procedurer for behandling, opbevaring og destruktion af inddatamateriale.	Ingen væsentlige afvigelser konstateret.
7	Kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles. Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for. Der må endvidere autoriseres personer, for hvem adgang til oplysninger er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.	Vi har forespurgt til procedure for styring af adgang, og vi har inspiceret proceduren. Vi har stikprøvevis inspiceret dokumentation for, at procedurerne er fulgt, og at der tages stilling til, hvorvidt adgang tildeles efter arbejdsbetinget behov.	Ingen væsentlige afvigelser konstateret.
8	Der skal træffes foranstaltninger for at sikre, at kun autoriserede brugere kan få adgang, og at disse kun kan få adgang til de personoplysninger og anvendelser, som de er autoriserede til.	Vi har forespurgt til foranstaltninger til begrænsning af uautoriserede adgange, og vi har stikprøvevis inspiceret de implementerede foranstaltninger.	Ingen væsentlige afvigelser konstateret.

Kontrol-nr.	Kontrolmål	Revisionshandlinger	Resultat
9	Uddatamateriale må kun anvendes af personer, der er beskæftiget med de formål, til hvilke behandlingen af personoplysningerne foretages. Herudover må uddatamateriale anvendes af personer, som er beskæftiget med revision eller drifts- og systemtekniske opgaver i det pågældende system. Uddatamateriale skal opbevares på en sådan måde, at uvedkommende ikke kan få adgang til at gøre sig bekendt med de personoplysninger, som er indeholdt heri. Uddatamateriale skal slettes eller tilintetgøres, når det ikke længere skal anvendes til de formål, som behandlingen varetager, og senest efter en af den dataansvarlige myndighed nærmere fastsat frist. Ved tilintetgørelse af uddatamateriale skal der træffes de fornødne sikkerhedsforanstaltninger mod, at materialet misbruges eller kommer til uvedkommendes kendskab. Bestemmelserne i stk. 1-5 gælder ikke for uddatamateriale, som indgår i en manuel sag eller i et manuelt register.	Vi har forespurgt til behandling af persondata i uddata. Vi har forespurgt til politik for destruktion og opbevaring af uddata, og vi har inspiceret politikken og autorisation af adgange til uddatamateriale.	Ingen væsentlige afvigelser konstateret.
10	Der må kun etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.	Vi har forespurgt til sikring af kommunikationsforbindelser, og vi har inspiceret dokumentation for anvendelse af Datatilsynets definition af stærk kryptografi.	Ingen væsentlige afvigelser konstateret.
11	Bestemmelserne i kapitel 3 finder ikke anvendelse i det omfang, de behandlede oplysninger ikke i sig selv ville være omfattet af anmeldelsespligt til Datatilsynet.	Ikke relevant, idet Fonden Center for Autisme ikke er anmeldelsespligtige til Datatilsynet.	Ingen væsentlige afvigelser konstateret.
12	Autorisationer, jf. § 11, skal angive, i hvilket omfang brugeren må forespørge, inddatere eller slette personoplysninger.	Vi har forespurgt til differentiering af rettigheder i forhold til inddatering og sletning, og vi har inspiceret dokumentation for differentiering af rettigheder.	Ingen væsentlige afvigelser konstateret.

Kontrol-nr.	Kontrolmål	Revisionshandlinger	Resultat
13	Det skal sikres, at de autoriserede personer fortsat opfylder betingelserne i § 11, stk. 2 og 3, og § 16. Kontrol heraf skal foretages mindst en gang hvert halve år.	Vi har forespurgt til periodisk gennemgang af adgange, og vi har stikprøvevis inspiceret dokumentation for, at gennemgangen er foretaget. Vi har forespurgt til kontrol for periodisk gennemgang.	Ingen væsentlige afvigelser konstateret.
14	Der skal foretages registrering af alle afviste adgangsforsøg. Hvis der inden for en fastsat periode er registreret et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg fra samme arbejdsstation eller med samme brugeridentifikation, skal der blokeres for yderligere forsøg. Der skal løbende ske opfølgning i myndigheden.	Vi har forespurgt til låsning af brugerkonti efter et givent antal fejlforsøg, og vi har inspiceret dokumentation for sikring af, at konti låses efter et givent antal fejlforsøg. Vi har forespurgt til notifikation i forbindelse med låsning af brugerkonti, og vi har inspiceret dokumentation for notifikation.	Ingen væsentlige afvigelser konstateret.
15	Der skal foretages maskinel registrering (logning) af alle anvendelser af personoplysninger. Registreringen skal mindst indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes. Myndigheder med et særligt behov kan opbevare loggen i op til 5 år. Bestemmelsen i stk. 1 finder ikke anvendelse for personoplysninger, som indgår i tekstbehandlingsdokumenter og lignende, der ikke foreligger i endelig form. Det samme gælder sådanne dokumenter, som foreligger i endelig form, hvis der sker sletning inden for en af den dataansvarlige myndighed nærmere fastsat kortere frist. Bestemmelsen i stk. 1 finder ikke anvendelse, hvis behandlingen af personoplysninger udelukkende sker ved afvikling af programmer, som foretager en foruddefineret massebehandling af personoplysninger (”batch”-kørsler). Der skal dog foretages maskinel logning af	Vi har forespurgt til logning af behandling af persondata, og vi har inspiceret den opsatte logning. Vi har forespurgt til interne bestemmelser for sletning af logfiler. Vi har forespurgt til kontrol for sletning af logfiler, og vi har inspiceret den implementerede kontrol.	Ingen væsentlige afvigelser konstateret.

Kontrol-nr.	Kontrolmål	Revisionshandlinger	Resultat
	bruger og tidspunkt for behandlingen. Bestemmelsen i stk. 1 finder endvidere ikke anvendelse, hvis behandlingen af personoplysningerne udelukkende sker med henblik på statistiske eller videnskabelige undersøgelser, og identifikationsoplysningerne forinden enten er krypteret eller erstattet med et kodenummer eller lignende. Der skal dog foretages maskinel logning af bruger og tidspunkt for behandlingen. Bestemmelsen i stk. 1 finder endelig ikke anvendelse for personoplysninger, som i form af måle- eller analyseresultater automatisk lagres i medicoteknisk udstyr. Undtagelsen omfatter tillige personoplysninger, som manuelt registreres i medicoteknisk udstyr til supplering af automatisk lagrede oplysninger.		