Sønderup + Partnere
Registrerede Revisorer FSR

Bellcom Hosting ApS

Uafhængig revisors ISAE 3000-erklæring med høj sikkerhed om foranstaltninger til styring af risici i relation til net- og informationssystemer og rapporteringsforpligtelser i henhold til aftale med Bellcom Hosting ApS' kunder

For perioden 23.12.2023 – 18.12.2024

Indholdsfortegnelse

Ledelsens udtalelse

Bellcom Hosting ApS leverer tjenester til Bellcom Hosting ApS' kunder i henhold til Databehandleraftale med Valgsted / OS2dagsorden / OS2forms / Consul.

Medfølgende beskrivelse er udarbejdet til brug for Bellcom Hosting ApS' kunder, der har anvendt Bellcom Hosting ApS tjenester vedrørende Valgsted / OS2dagsorden / OS2forms / Consul, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som Bellcom Hosting ApS' kunder selv har udført ved vurdering af, om kravene til sikring af et højt cybersikkerhedsniveau i henhold til gældende lovgivning er overholdt.

Bellcom Hosting ApS anvender Hetzner GmbH som NIS2-serviceunderleverandør vedr. Hosting og backup. Erklæringen anvender helhedsmetoden og omfatter kontroller, som Hetzner GmbH varetager for Bellcom Hosting ApS.

Enkelte af de kontrolmål, der er anført i Bellcom Hosting ApS beskrivelse side 18-33, kan kun nås, hvis de komplementære kontroller hos Bellcom Hosting ApS kunder er hensigtsmæssigt designet, implementeret og operationelt effektive sammen med Bellcom Hosting ApS kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af design, implementering og operationel effektivitet af disse komplementære kontroller.

Bellcom Hosting ApS bekræfter, at:

a) Den medfølgende beskrivelse, side 8-17, giver en hensigtsmæssig præsentation af Valgsted / OS2dagsorden / OS2forms / Consul, der har været anvendt af Bellcom Hosting ApS' kunder i hele perioden fra 23. december 2023 - 18. december 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan Valgsted / OS2dagsorden / OS2forms / Consul, var designet og implementeret, herunder redegør for:

   - De typer af tjenester, der er leveret
   - De processer i net- og informationssystemer, der er anvendt til at levere tjenesterne
   - Hvordan net- og informationssystemer behandler andre betydelige begivenheder end de der direkte vedrører levering af tjenester
   - De processer, der i tilfælde af brud på sikkerheden vedrørende tjenester understøtter, at Bellcom Hosting ApS' kunder kan foretage anmeldelse til tilsynsmyndigheden
   - De processer, der er rettet mod begivenheder, der kan være til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer
   - Relevante kontrolmål og kontroller designet og implementeret til at nå disse mål
   - Komplementære kontroller, som vi med henvisning til Valgsted / OS2dagsorden / OS2forms / Consul's afgrænsning har forudsat ville være implementeret af Bellcom Hosting ApS' kunder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen

- Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for levering af tjenester

(ii) Indeholder relevante oplysninger om væsentlige ændringer ved Valgsted / OS2dagsorden / OS2forms / Consul, foretaget i perioden fra 23. december 2023 - 18. december 2024.

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af Valgsted / OS2dagsorden / OS2forms / Consul under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og derfor ikke kan omfatte ethvert aspekt ved Valgsted / OS2dagsorden / OS2forms / Consul, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var efter vores vurdering hensigtsmæssigt designet, implementeret og operationelt effektive i hele perioden fra 23. december 2023 - 18. december 2024. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 23. december 2023 - 18. december 2024

c) Der er etableret og opretholdt passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer med henblik på at levere tjenester til Bellcom Hosting ApS' kunder samt for at forhindre hændelser eller minimere deres indvirkning.

I relation til ovenstående vurderinger bemærkes, at reguleringen vedrørende krav til sikkerheden i net- og informationssystemer er ny og kompleks. Der har endnu ikke på alle områder udviklet sig en konsistent praksis for, hvordan de enkelte regler skal fortolkes. Selvom det er vores vurdering, at vi har etableret og opretholdt passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger, kan der således vise sig at være forhold, hvor myndigheder og samarbejdspartnere anlægger en anden vurdering.

Kolding d. 20. december 2024

Bellcom Hosting ApS
Bredgade 20 – 1
6000 Kolding

Jørn Skifter Andersen
Partner

Linda Skov
Direktør og partner

Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med høj sikkerhed om foranstaltninger til styring af risici i relation til net- og informationssystemer og rapporteringsforpligtelser i henhold til aftale med Bellcom Hosting ApS' kunder

Til: Bellcom Hosting ApS og Bellcom Hosting ApS' kunder

Omfang

Vi har fået som opgave at afgive erklæring om Bellcom Hosting ApS's beskrivelse på side 8-17 af identifikation af behandling Valgsted / OS2dagsorden / OS2forms / Consul i henhold til databehandleraftale med Bellcom Hosting ApS´ kunder (Dataansvarlig), i hele perioden fra 23. december 2023 - 18. december 2024 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Nærværende erklæring omfatter, om Bellcom Hosting ApS har designet og implementeret hensigtsmæssige kontroller, der knytter sig til de kontrolmål, der fremgår side 18-33, og om disse kontroller har været operationelt effektive i perioden 23. december 2023 - 18. december 2024. Erklæringen omfatter ikke en vurdering af Bellcom Hosting ApSs generelle efterlevelse af kravene i EU's direktiv om "Foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen".

Bellcom Hosting ApS anvender Hetzner GmbH som NIS2-serviceunderleverandør for Valgsted / OS2dagsorden / OS2forms / Consul. Erklæringen anvender helhedsmetoden og omfatter kontroller, som Hetzner GmbH varetager for Bellcom Hosting ApS.

Enkelte af de kontrolmål, der er anført i Bellcom Hosting ApS beskrivelse side 8-17, kan kun nås, hvis de komplementære kontroller hos Bellcom Hosting ApS kunder er hensigtsmæssigt designet, implementeret og operationelt effektive sammen med Bellcom Hosting ApS kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af design, implementering og operationel effektivitet af disse komplementære kontroller.

Vores konklusion udtrykkes med høj sikkerhed.

Bellcom Hosting ApS's ansvar

Bellcom Hosting ApS er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de tjenester, beskrivelsen omfatter; for at fastlægge kontrolmålene samt for at designe, implementere og effektivt operere kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

Vores revisionsfirma anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Bellcom Hosting ApS's beskrivelse samt om design, implementering og operationel effektivitet af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 (ajourført), "Andre erklæringer med sikkerhed end revision eller review af historiske finansielle oplysninger", og de yderligere krav, der er gældende i Danmark, med henblik på at opnå begrænset sikkerhed for, at beskrivelsen i alle væsentlige henseender er hensigtsmæssigt præsenteret, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt designet, implementeret og operationelt effektive.

En erklæringsopgave med begrænset sikkerhed om at afgive erklæring om beskrivelsen, design, implementering og operationel effektivitet af kontroller hos en NIS2-serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i NIS2-serviceleverandørens beskrivelse af sin tjeneste samt for kontrollernes design, implementering og operationelle effektivitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er hensigtsmæssigt præsenteret, og at kontrollerne ikke er hensigtsmæssigt designet, implementeret og operationelt effektive. Vores handlinger har omfattet analyser, forespørgsler og andre handlinger med henblik på at opnå begrænset sikkerhed for vores vurdering af den operationelle effektivitet af sådanne kontroller, som vi anser for nødvendige for at give begrænset sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med begrænset sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt relevans af de kriterier, som NIS2-serviceleverandøren har specificeret og beskrevet side 3-4.

Handlingerne i en opgave med begrænset sikkerhed varierer i art og tidsmæssig placering fra, og har mindre omfang end, en opgave med høj grad af sikkerhed. Som følge heraf er den grad af sikkerhed, der er for vores konklusion, betydeligt mindre end den sikkerhed, der ville være opnået, hvis der var udført en erklæringsopgave med høj grad af sikkerhed.

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

Begrænsninger i kontroller hos en NIS2-serviceleverandør

Bellcom Hosting ApS's beskrivelse er udarbejdet for at opfylde de almindelige behov hos Bellcom Hosting ApS' kunder og omfatter derfor ikke nødvendigvis alle de aspekter ved tjenesterne og kontrol aktiviteter i tilknytning hertil, som Bellcom Hosting ApS' kunder måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en NIS2-serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle brud på cybersikkerheden. Herudover er fremskrivningen af enhver vurdering af den operationelle effektivitet til fremtidige perioder undergivet risikoen for, at kontroller hos en NIS2-serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i ledelsens udtalelse. Under vores arbejde er vi ikke blevet bekendt med forhold, der giver os anledning til at konkludere,

(a) at beskrivelsen af Valgsted / OS2dagsorden / OS2forms / Consul, således som disse var designet og implementeret i perioden 23. december 2023 til 18. december 2024, ikke i alle væsentlige henseender er hensigtsmæssigt præsenteret, og

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, ikke i alle væsentlige henseender var hensigtsmæssigt designet og implementeret i perioden 23. december 2023 til 18. december 2024, og

(c) at de vurderede kontroller, ikke har været operationelt effektive i perioden 23. december 2023 til 18. december 2024

Beskrivelse af vurdering af kontroller

De specifikke kontroller, der blev vurderet, samt arten, den tidsmæssige placering og resultaterne af disse vurderinger, fremgår af side 18-33.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af vurdering af kontroller i afsnit 4 er udelukkende tiltænkt Bellcom Hosting ApS' kunder, der har anvendt Bellcom Hosting ApS's Valgsted / OS2dagsorden / OS2forms / Consul. Vi har lagt til grund, at Bellcom Hosting ApS' kunder har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som Bellcom Hosting ApS' kunder selv har udført, ved vurdering af, om kravene til sikring af et højt cybersikkerhedsniveau, i henhold til gældende lovgivning, er overholdt.

Kolding d. 20. december 2024

Sønderup & Partnere A/S
registrerede revisorer FSR
CVR-nr. 27905072

Palle Lysbjerg
Registreret revisor
mne18078

Bellcom Hosting ApS' beskrivelse af Valgsted / OS2dagsorden / OS2forms / Consul

Bellcom Hosting ApS

Bellcom hoster alle sine løsninger hos en underdatabehandler, Hetzner GmbH i Tyskland. Vi sikrer at alle servere er oprettet på lokationer indenfor EU samt at ekstra backup tages til en anden lokation i Tyskland.

Hetzner GmbH tilbyder et professionelt og sikkert datacenter og dækker alle vore krav til en professionel hosting udbyder såsom overvågning, strømbackup og brandslukning. Serverne er stadig bygget, så det hurtigt og nemt kan reetableres eller udbygges.

I Bellcom har vi gennem vores erfarne medarbejdere en meget bred viden indenfor IT. Vi kommer fra forskellige IT- og teknikerhverv, hvor arbejdet har været præget af problemløsning og styring af projekter, og vi er derfor godt rustet til at rådgive kunderne omkring totale løsninger fra A til Z.

Organisation og ansvar

Bellcom er inddelt i afdelingerne IT-drift, Udvikling og Support. Alle supportopgaver varetages af support-afdelingen. IT-drift har ansvaret for drift, vedligeholdelse og videreudvikling af vores hostingmiljø. Ledelsen hos Bellcom har det overordnede ansvar for IT-sikkerheden i virksomheden.

Valgsted / OS2dagsorden / OS2forms / Consul behandling af personoplysninger

Behandling af personoplysninger

For Valgsted behandles almindelige personoplysninger, oplysninger om politisk overbevisning samt cpr-nr. for valgstyrere ved offentlige valg i kommunerne, tilforordnede vælgere ved offentlige valg i kommunerne samt administrativt personale og øvrigt servicepersonale ved offentlige valg i kommunerne.

For OS2dagsorden behandles udelukkende almindelige personoplysninger vedr. administrativt personale og øvrigt servicepersonale hos kunden.

For OS2forms behandles almindelige personoplysninger, samt mulighed for alle typer af personfølsomme oplysninger.

For Consul behandles almindelige personoplysninger, cpr-nr, cvr-nr samt e-mail adresser.

Beskrivelse af kontroller for drift af GDPR platforme

Introduktion

Formålet med denne beskrivelse er at levere information til Bellcom's kunder, og deres revisorer, vedrørende kravene i den internationale revisionsstandard for erklæringsopgaver om kontroller hos en serviceleverandør, ISAE 3000.

Beskrivelsen har herudover det formål, at give information om de kontroller, der er anvendt for vores hostingsystem.

GDPR Servere

Følgende beskrivelse omfatter de kontrolmål og kontroller hos Bellcom, som omfatter størstedelen af vores kunder og er baseret på vores standardleverance. Individuelle kundeforhold, er ikke medtaget i denne beskrivelse.

Platformen OS2dagsorden

OS2dagsorden giver papirløse møder. Løsningen erstatter papirreferater, papirdagsordner, mv., til møderne i kommuner.

Løsningen er open source, og den virker uafhængigt af platforme og styresystemer. OS2dagsorden fungerer på alle PCer og tablets med internet.

Med OS2dagsorden får den enkelte mødedeltager et overblik og indsigt i al dokumentation vedr. en aktuel mødeaktivitet og er særdeles passende til alle former for bestyrelses-, formandskab og udvalgsarbejde. En mødedeltager får herigennem mulig for at gøre egne noter og talebreve, som hæfter sig til enten den samlede dagsorden eller helt ned på bilagsniveau.

Brugeren for evnen til at gennemse historiske møder og en samlede orientering om aktuelle og udvalgte mødeaktiviteter alt efter den pågældende brugers rolle og/eller rettigheder.

OS2dagsorden giver der ud over en administrativ gevinst i planlægning og elektronisk distribution af al mødedata.

OS2dagsorden er blevet til for at lette både brugere og administration om fremtidig mødeplanlægning og indsigt.

OS2dagsorden opererer med 3 sikkerhedsniveauer. Åbne data, lukke data og personfølsomme data. I løsningen er der indbygget logning af adgangen til alle data i henhold til retningslinjerne fra Datatilsynet.

Platformen Valgsted

Der skal mange til for at få et valg til at køre som smurt. Her kommer Valgsted ind i billedet. Valgsted er et webbaseret system til at håndtere bemandingen på valgstederne. Det kunne være valgstyrere, tilforordnede og frivillige, der er nødvendig for afholdelsen af valg. De medvirkende og partierne kan tilmelde sig og koordinere i Valgsted, og de kan brug Valgsted til at kommunikere med valgsekretariatet.

Valgsted er for valgsekretariatet, der kan skabe sig et overblik over hvor mange tilforordnede, som de skal bruge hvert enkelt sted, og hvor mange der har meldt sig i alt.

Valgsted løfter en tung, manuel opgave. Løsningen er en automatisering, der giver valgsekretariatet og partiforeninger overblikket over opgaven og fastholder et højt datasikkerhedsniveau.

Platformen Valgsted indeholder blandt andet CPR numre. I løsningen er der indbygget logning af adgangen til alle data i henhold til retningslinjerne fra Datatilsynet. Al tilgang til løsningen foregår via Single Sign On og 2 faktor godkendelse.

Platformen OS2forms

OS2forms er et formularværktøj til at gøre selvbetjeningsløsninger automatiske og digitale.

En løsning der kan bruge til at skræddersy digitale selvbetjeningsløsninger til glæde for borgere, virksomheder og medarbejdere. OS2forms er et Open Source alternativ til kommercielle selvbetjeningsværktøjer.

Med automatisering af indsamlingen af formulardata bliver arbejdet endnu mere effektivt.

Platformen OS2forms indeholder blandt andet CPR numre. I løsningen er der indbygget logning af adgangen til alle data i henhold til retningslinjerne fra Datatilsynet.

Platformen Consul

Consul er en smidig og let tilgængelig løsning, der understøtter den demokratiske beslutningsproces i kommunerne ved at inddrage borgerne aktivt i alle faser, efter behov.

Løsningen skaber gennemsigtighed og indflydelse på kommunale beslutninger for borgerne. Den gør processen nem og effektiv og giver samtidigt et overblik over stadierne i f.eks. et borgerbudget. Gennem samarbejde med borgerne opnås en større effektivitet i beslutningsprocessen.

Integration til NemLog-in er med til at bekræfte borgernes identitet, men lader også borgeren følge sine egne bidrag og indsendelser. Via NemLog-in kan løsningen lave opslag på, om borgeren bor i kommunen og sikrer dermed, at man kun kan bidrage, hvis man har bopæl i kommunen.

Consul dækker følgende behov:

- Borgerforslag
- Borgerbudgetter
- Meningsmålinger
- Politikudvikling
- Debat

Sikkerhedsopdateringer

I Bellcom har vi sat sikkerhedsopdateringerne i system. For personfølsomme løsninger er det muligt at tegne en GDPR+ aftale hvor vi automatisk opdaterer løsningerne lige så snart der frigives sikkerhedsrettelser. Først efter opdateringen testes løsningen. Hvorved data er sårbare i mindst mulig tid.

http://bellcom.dk/gdpr

Kildekode

For alle Bellcom's løsninger gælder det at koden for projekter vi arbejder på styres via et eksternt versionsstyringssystem. Koden er derfor tilgængelig for kunderne via github.com/bellcom

Organisation og ansvar

Bellcom er inddelt i afdelingerne IT-drift, Udvikling og support. Alle support opgaver varetages af support afdelingen. IT-drift har ansvaret for drift, vedligeholdelse og videreudvikling af vores hostingmiljø.

Ledelsen hos Bellcom har det overordnede ansvar for IT-sikkerheden i virksomheden.

Risikostyring i Bellcom

Vi har procedurer for løbende risikovurdering af vores forretning og specielt vores hosting ydelser. Dermed kan vi sikre, at de risici, som er forbundet med de services og ydelser, vi stiller til rådighed, er minimeret til et acceptabelt niveau.

Medarbejderne gennemgår og underskriver en vejledning i generel sikkerhedsdatahåndtering samt kodeords skift hver tredje måned.

IT-afdelingen følger et "årshjul" med hensyn til gennemgang af adgange, sikkerhedsopdateringer m.v.

Ansvaret for risikovurderinger er placeret hos IT-driften, og skal efterfølgende forankres og godkendes hos Bellcom ledelse.

Generelt om vores kontrolmål og implementerede kontroller

Vores overordnede kontrolmål er at sikre, at de politikker vi har angivet i vores samlede informationssikkerhedspolitik, efterleves. Herunder især i forhold til de registrerede.

Vores metodik til implementering af kontroller er defineret ud fra ISO 27002:2013 regelsættet for styring af informationssikkerhed.

Vi foretager løbende forbedringer af både politikker, procedurer og den operationelle drift. Vi foretager årlig revidering af, hvorvidt vi lever op til vores regelsæt, der centrerer sig om, hvordan vi leverer vores driftsydelser, foretager genetablering, håndterer sikkerhedsopdatering mv.

Bellcom benytter sig alene af én underleverandører i forbindelse med opbevaring af en kopi af den samlede backup. Der stilles krav om at denne underleverandører besidder en gyldig ISAE 3402 lignende revisorerklæring. (ISO/IEC 27001:2013 certificate)

Kontrolmiljø

Det følgende beskriver vores kontrolmiljø nærmere for hvert enkelt område.

Overordnede retningslinjer

Vi har defineret vores overordnede metodik og tilgang til levering af vores ydelser med hvad dette indebærer, i vores IT-sikkerhedspolitik og tilhørende strategiske og taktiske dokumenter. Formålet er at sikre, at vi har ledelsesgodkendte retningslinjer for informationssikkerhed i forhold til forretningsstrategien - og i forhold til relevant lovgivning. Ledelsens budskab er kommunikeret til alle medarbejdere i Bellcom, og vi opdaterer løbende dokumenterne efter behov, og minimum en gang årligt.

Hændelseshåndtering og informationssikkerhedsbrud

Beredskabsplanen er den overordnede plan for håndtering af brud på informationssikkerheden. En uforudset hændelse kan være forsøg på hacking af en server, uautoriseret adgang til en server m.m. I forbindelse med en sådan hændelse skal det vurderes om der også er et informationssikkerhedsbrud, hvilket gøres af beredskabsledelsen.

Informationssikkerhedsbrud

Er en identificeret forekomst af en system-, tjeneste- eller netværkstilstand, der indikerer et muligt brud på informationssikkerhedspolitikken eller svigt af kontroller, eller en tidligere ukendt situation, der kan være relevant for sikkerheden.

Under informationssikkerhedsbrud hører brud på persondatasikkerheden gennem, hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet

Orientering af kunder

Ved aktivering af beredskabet orienteres alle berørte kunder direkte eller via Bellcom's drifts nyhedsbrev. Orienteringen skal indeholde:

- En kort beskrivelse af problematikken
- De aktive handlinger der nu foretages for udbedring
- Forventet udbedringstid
- Tidspunktet for næste orientering (hver 4 time inden for normal arbejdstid eller næste morgen)

Skaden ved sikkerhedsbrud skal holdes på et acceptabelt niveau. Målet opnås ved at der fastlægges reaktionsprocedurer for kendte og hyppige sikkerhedshændelser, så de kan håndteres hurtigt og effektivt og ikke udvikler sig. Der skal desuden opretholdes et it-beredskab i tilfælde af større hændelser, som ikke kan håndteres med de normale reaktionsprocedurer.

Hændelser og svagheder skal registreres og årligt rapporteres til beredskabsledelsen. Disse registreres i følgende løsning. https://kunde.bellcom.dk/im

Ved alvorlige hændelser skal der foretages en efterfølgende evaluering af hændelsen, som behandles I beredskabsledelsen. Registrering af hændelser hjælper til at finde den optimale balance imellem forebyggende, opdagende og udbedrende foranstaltninger.

I tilfælde af et informationssikkerhedsbrud udføres følgende:

- Der sendes en email til informationssikkerhedskoordinatoren (ISK) hg@bellcom.dk (Driften / Udvikler team)
- Hændelsen oprettes i kunde.bellcom.dk/im som værende "ikke løst" og orienterer Beredskabsledelsen
- Sikkerhedsbruddet stoppes. (driften)
- Logfiler og andet relevant for efterfølgende undersøgelse af hændelsen indsamles (driften)
- Forslag til fremadrettet forebyggelse forelægges beredskabsledelsen. (driften)

- Kunden orienteres om hændelsen såfremt dette er påkrævet (beredskabsledelsen)
- Vurdering af om hændelsen skal indberettes til Datatilsynet som et brud på brud på databeskyttelseslovgivningen (beredskabsledelsen)
- Alt relevant materiale gemmes i en zip fil og sendes til informationssikkerhedskoordinatoren
- Zip filen lægges op på opgaven i kunde.bellcom.dk/im og denne lukkes (ISK)

Rapportering af informationssikkerhedsbrud

Alle medarbejdere har pligt til at rapportere sikkerhedsbrud til informationssikkerhedskoordinatoren.

Alle medarbejdere og eksterne kontrahenter har pligt til at rapportere observerede svagheder eller sårbarheder i it-systemer og it-services til informationssikkerhedskoordinatoren.

Kontrakter, SLA

Vi tilbyder kontrakter på hostingydelser for vores kunder. Særlige forhold er beskrevet heri, som de var ved aftaleindgåelse.

Vores SLA (Service Level Agreement) beskriver vores generelle vilkår, i forbindelse med vores ydelse overfor vores kunder, responstid, support mv.

Bellcom tilbyder Opdaterings aftaler hvor vi påtager os det fulde ansvar for opdateringer af løsninger og efterfølgende test. Se http://bellcom.dk/gdpr

Medarbejdersikkerhed

Formål

Vi vil sikre, at alle i virksomheden er bekendte med deres roller og ansvar - herunder også vores underleverandører og 3. parter, og at alle er kvalificerede og egnede til at udføre deres rolle.

Roller og ansvar og samarbejde med eksterne

Alle i vores virksomhed skal leve op til den rolle, som er tilegnet dem samt følge vores procedurer jf. vores IT-sikkerhedspolitik samt ansvars- og rollefordeling. Dette er for at sikre, at bl.a. sikkerhedsrelaterede forhold eskaleres og håndteres. Vigtigst er, at vi passer på vores kunders data, vores udstyr og dermed vores forretning. Rolle- og ansvarsbeskrivelsen, herunder opgaver og ansvar i forhold til sikkerheden, er defineret i de udarbejdede rollebeskrivelser, medarbejdernes ansættelseskontrakt samt i IT-sikkerhedspolitikken.

Vi har procedurer for ansættelse af medarbejdere og etablering af samarbejde med eksterne, hvor vi sikrer, at vi ansætter den rigtige kandidat ift. baggrund og kompetence. Vi har rolle- og ansvarsbeskrivelser for medarbejdere og medarbejderkategorier, så alle er bekendte med deres ansvar.

Ansættelsesvilkår

Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt, hvor forhold omkring alle sider af ansættelsen, herunder ophør og sanktioner ved evt. sikkerhedsbrud, er angivet.

Fysisk sikkerhed

Formål

Vi vil sikre, at vi har et betryggende fysisk miljø omkring Bellcom og dermed vores kunders data. Servere, services, data og informationer generelt er afskærmet mod miljømæssige påvirkninger (brand, vand, temperatur mv.), og herudover skal vi have fornøden og betryggende sikring mod hærværk, tyveri mv.

Hosting / datacenter

Bellcom hoster sine løsninger hos Hetzner GmbH. Adgangen hertil sker via en "management console" som tilgås via nettet. I vore processer kontrollerer vi, at underleverandøren overholder alle kravene for en ISAE-3000 erklæring. Hetzner GmbH er ISO/IEC 27001:2013 certificeret. Centeret er sikret mod brand, oversvømmelser, indbrud, strømsvigt, overophedning og har batteri og generator som nødstrømsanlæg.

Bellcom sikrer, at de fornødne erklæringer om dette er hjemhentet og godkendt via ISO / TUV certificeringer.

Da Bellcom tilbyder hosting af løsninger med garanteret datasikkerhed 24-7 og med tilgængelighed inden for almindelig arbejdstid, er det afgørende, at datacenteret er sikret mod alle forudsebare risici, samt at der er en nødplan, der kan iværksættes indenfor få timer eller dage i tilfælde af helt uforudsete og usandsynlige hændelser.

Serverrum (udfaset i erklæringsperioden)

Bellcoms datacenter er beliggende på særskilt lokation på Dalbygade 40H, 6000 Kolding.

Rummet ligger i et kompleks sammen med andre lejere, og adgang til bygningskomplekset sker med nøgle udenfor åbningstid.

Adgang til forrummet sker med brik og nøgle. Her er hylde- og arbejdsplads med mulighed for opkobling af PC. Uautoriseret adgang (dvs. uden brug af brik) giver alarm til Dansikring.

Selve serverrummet er en klima- og brandbeskyttet "bygning i bygningen". Adgang hertil sker med brik og kode. Autoriseret adgang hertil udløser SMS til driftsleder og driftsteam, og der sker fotodokumentation af, hvem der er i rummet (konstant fotoovervågning af døren til rummet indefra).

Serverrummet er forsynet med CTS kontrolsystem (teknik- og miljøvagt), eltavle, tre serverskabe med fysiske diske (konfigureret som virtuelle servere med redundans), kommunikationscontrollere, to firewalls (1 redundant), tre UPS, tre klimaanlæg, vandalarmer (gulv, kølekondens og tag) samt brandalarm med Inergen brandslukningsanlæg. Desuden er der egen nødstrømsgenerator på adressen. Alle systemer og sensorer overvåges af CTS, og overvågningsdata logges direkte samt på server (med backup). CTS kan fjernovervåges fra Bredgade 20 på cts.bellcom.dk.

Da Bellcom tilbyder hosting af løsninger med garanteret datasikkerhed 24-7 og med tilgængelighed inden for almindelig arbejdstid, er det afgørende, at datacenteret er sikret mod alle forudsebare risici, samt at der er en nødplan, der kan iværksættes indenfor få timer eller dage i tilfælde af helt uforudsete og usandsynlige hændelser.

Kontorer

Adgangen til kontoret beliggende Bredgade 20, sker via fælles hovedindgang, der deles med lejeren i stueetagen (Cortex). Herfra sker adgangen til Bellcoms trappeopgang via aflåselig dør, og indgangen til kontoret sker via endnu en aflåselig dør. Kontoret er desuden sikret af tyverialarm hvor hver medarbejder har sin egen kode.

Adgangen sker via storrumskontor, således at uvedkommende ikke uopdaget kan få adgang. Ved møder, frokost etc., hvor døren er ubevogtet, låses den.

Hjemmearbejde

Vi har etableret mulighed for, at vores medarbejdere kan arbejde hjemmefra af hensyn til bl.a. Driftsvagt. Adgang til fjernarbejde sker alene via VPN til Bellcom's kontorer og herfra videre til hosting centeret.

Sletning

Alle servere og tilhørende diske hos Hetzner GmbH slettes ved ophør af brugen af de anførte systemer.

Styring af netværk og drift

Formål

Vi vil sikre, at vores organisering af implementering, drift og ændring i og af vores ydelse sker struktureret og efter aftale med vores kunder. Vi skal sikre at IT-sikkerheden, generelt er høj, og via systemer og procedurer til sikring heraf, ikke kompromitter vores, vores kunders systemer og data. Vi skal have procedurer for genskabelse af data, overvågning og logning af data, og vi skal generelt have opmærksomhed på fortroligheden omkring vores kunders data.

Drift

Vi vil sikre at vores drift er stabil, korrekt og sikker. Gennem løbende dokumentation og processer sikrer vi at kunne udelukke eller minimere nøglepersonsafhængighed. Opgaver tildeles og fastsættes via procedurer for styring af den operative drift.

Ændringshåndtering

Vi har defineret en proces for ændringshåndtering, for at sikre, at ændringer sker efter aftale med kunder, og er tilrettelagt hensigtsmæssigt i forhold til interne forhold. Større ændringer sker alene baseret på en klassificering af opgaven, kompleksiteten og vurdering af påvirkning af andre systemer.

Ved større og/eller forretningskritiske ændringer, sikres det altid, som minimum, at;

- Alle ændringer drøftes, prioriteres og godkendes af ledelsen
- Alle ændringer testes
- Alle ændringer godkendes før idriftsættelse
- Alle ændringer idriftsættes på et fastsat tidspunkt, efter aftale med forretningen og/eller kunden
- Der fortages fall back-planlægning, som sikrer, at ændringer kan rulles tilbage eller annulleres, hvis den ikke fungerer
- Systemdokumentationen opdateres med den nye ændring, såfremt det vurderes nødvendigt

Vores miljø er altid opdelt logisk, i test og produktion, hvorved vi sikrer, at have testet et produkt eller ændring, før den kommer i produktion.

Underleverandører

Hvor vi bruger underleverandører fører vi tilsyn med disse. Bellcom benytter Hetzner GMBH som underleverandør til hosting og backup af løsninger.

Sikkerhedskopiering

Vi sikrer at kunne genskabe systemer og data på hensigtsmæssig og korrekt vis, samt efter de aftaler, vi har med vores kunder.

Vi har etableret en testplan for verificering af, hvorvidt sikkerhedskopieringen fungerer samt en test af hvordan systemer og data i praktisk kan reetableres. Der føres en log over disse tests, således at vi kan følge op på om vi kan ændre på procedurer og processer for at højne vores løsning.

Vi har defineret retningslinjer for på hvilken vis, vi foretager sikkerhedskopiering. Hver nat føres udvalgte data fra vores centrale systemer (i byen Falkenstein) til en anden lokation hos Hetzner GmbH (i byen Nuremberg) ved hjælp af vores backup-system. Dermed er data fysisk separeret fra vores driftssystemer.

En ansvarlig medarbejder får besked såfremt sikkerhedskopieringen ikke er sket, og foretager det fornødne hvis jobbet er fejlet, og logfører herefter dette.

Netværkssikkerhed

IT-sikkerheden omkring systemers og datas ydre rammer, er netværket mod internettet, remote eller lignende. Vi mener, at have sikret data og systemer også inde i netværket, men det ydre værn mod uvedkommende adgang er af højeste prioritet hos os.

Adgang til vores systemer fra vores kunder, sker via de offentlige netværk.

Alene godkendt netværkstrafik (indgående) kommer gennem vores firewall.

Vi er ansvarlige for driften og sikkerheden hos os, dvs. fra og med systemerne hos os og ud til internettet. Vores kunder er selv ansvarlige for at kunne tilgå internettet.

Håndtering af databærende medier

Vi skal sikre, at vores og vores kunders systemer og data beskyttes. Vi håndterer derfor ikke kunders data på håndbårne medier (Eksterne USB medier, CD/DVD) uden forudgående skriftlig aftale med kunderne samt ved passende fysisk beskyttelse mod miljømæssige på- virkninger (varme mv.) samt hærværk og tyveri.

Alt databærende udstyr (USB, CD/DVD, harddiske mv.) destrueres inden bortskaffelse for at sikre, at data ikke er tilgængeligt.

Vores dokumentation opbevares på to af hinanden uafhængige lokationer. Dette sikrer tilgængeligheden af dokumentationen i tilfælde af f.eks. nedbrud.

Ekstern datakommunikation

Ekstern datakommunikation sker via e-mails, idet vores kunders adgang og brug af vores servere, ikke betragtes som ekstern datakommunikation. Yderligere kommunikation sker gennem vores support system samt vore projektplanlægnings værktøjer.

Glemte kodeord, personoplysninger, bestillinger mv. håndteres aldrig via telefon, udelukkende på skrift (opdelt på e-mail og SMS) og først efter vores medarbejdere har konstateret, at det er den korrekte og autoriserede person, vi har kontakt til.

Overvågning og logning

Vi har et overvågningssystem hvor vi overvåger drifts kritiske servere og udstyr. Vores driftsmedarbejdere foretager den daglige overvågning af vores systemer via måling af grænseværdier. Vi opsamler logs for alle servere og enheder i netværket.

Til styring af overvågning og opfølgning på hændelser, har vi implementeret formelle incident og problem management systemer der automatisk reagerer på grænseværdier og eskalerer hændelser. Driften modtager disse via e-mail samt sms.

Beredskabsplan

Formål

Vi vil have mulighed for at genoptage vores primære og centrale forretningsprocesser og systemer, efter en katastrofelignende situation.

Beredskabsplan

Skulle der opstå en nødsituation, har Bellcom udarbejdet en overordnet beredskabsplan. Beredskabsplanen er forankret i IT-risikoanalysen og vedligeholdes minimum årligt, i forlængelse af udførelsen af analysen. Planen testes 1 gang årligt som en del af vores overordnet beredskab, så vi sikrer, at kunderne i mindst muligt omfang vil opleve forstyrrelser i driften, i forbindelse med en eventuel nødsituation.

Planen og procedurerne er forankret i vores driftsdokumentation og procedurer.

Overensstemmelse med lovbestemte og kontraktlige krav

Vi er ikke underlagt særlig lovgivning i forhold til vores ydelse. Vores kunder kan dog være, og de steder, er vores understøttelse heraf aftalt særskilt.

Vi lader os årligt revidere af ekstern revisor, med henblik på afgivelse af erklæring for overholdelsen af kontrollerne, nævnt i denne beskrivelse.

Vi har en intern kontrol, hvor vi undersøger, om de etablerede politikker og retningslinjer overholdes af medarbejderne. Derudover har vi en kontrol der sikrer, at vores udstyr, såsom servere, databaser, netværksudstyr mm., er sat op jf. vores baselines.

Komplementerende kontroller der udføres af kunder hos Bellcom

Bellcom's kunder er, med mindre andet er aftalt, ansvarlige for at etablere forbindelse til Bellcom's' servere. Herudover er Bellcom's' kunder, med mindre andet er aftalt, ansvarlige for:

- At det aftalte niveau for backup dækker kundens behov
- At gennemføre periodisk gennemgang af kundens egne brugere
- At sikre serviceleverandøren får korrekt information om oprettelse og nedlæggelse af brugere
- At beskrive egen sletning

Kontrolmål, kontrolaktivitet, test og resultat heraf

Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Inspiceret, at procedurer er opdateret.	Ingen bemærkninger
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret ved en stikprøve på 7 behandlinger af personoplysninger, at disse foregår i overensstemmelse med instruks.	Ingen bemærkninger
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Inspiceret, at den dataansvarlige er underrettet i tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.	Ingen bemærkninger

Kontrolmål, kontrolaktivitet, test og resultat heraf

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Inspiceret, at procedurer er opdateret. Inspiceret ved en stikprøve på 7 databehandleraftaler, at der er etableret de aftalte sikringsforanstaltninger.	Ingen bemærkninger
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed. Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Inspiceret, at databehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Inspiceret, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.	Ingen bemærkninger
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus software. Inspiceret, at antivirus software er opdateret.	Ingen bemærkninger
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Inspiceret, at firewall er konfigureret i henhold til intern politik herfor.	Ingen kommentarer

Kontrolmål, kontrolaktivitet, test og resultat heraf

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Inspiceret netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering.	Ingen bemærkninger
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger. Inspiceret ved en stikprøve på 3 brugeres adgange til systemer og databaser, at de er begrænset til medarbejdernes arbejdsbetingede behov.	Ingen bemærkninger
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter: • OS2dagsorden • valgsted • OS2forms • consul	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering. Inspiceret, at der ved en stikprøve på 3 alarmer er sket opfølgning, samt at forholdet er meddelt de dataansvarlige i behørigt omfang.	Ingen bemærkninger

Kontrolmål, kontrolaktivitet, test og resultat heraf

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme. Inspiceret, at teknologiske løsninger til kryptering har været tilgængelige og aktiveret i hele erklæringsperioden. Inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail. Forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger i erklæringsperioden, samt om de dataansvarlige er behørigt orienteret herom.	Ingen bemærkninger
B.9	Der er etableret logning i systemer, databaser og netværk af følende forhold: • Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder • Sikkerhedshændelser omfattende: o Ændringer i logopsætninger, herunder deaktivering af logning o Ændringer i systemrettigheder til brugere o Fejlede forsøg på log-on til systemer, databaser og netværk Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang og opfølgning på logs. Inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret. Inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning. Inspiceret ved en stikprøve på af logfiler har det forventede indhold i forhold til opsætning, og at der er dokumentation for den foretagne opfølgning og håndtering af evt. sikkerhedshændelser. Inspiceret ved en stikprøve på at der er dokumentation for den foretagne opfølgning på aktiviteter udført af systemadministratorer og andre med særlige rettigheder.	Ingen bemærkninger

Kontrolmål, kontrolaktivitet, test og resultat heraf

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form. Inspiceret ved en stikprøve på 1 udviklings- og testdatabaser, at personoplysninger heri er pseudonymiseret eller anonymiseret. Inspiceret ved en stikprøve på 1 udviklings- og testdatabaser, hvor personoplysninger ikke er pseudonymiseret eller anonymiseret, at dette er sket efter aftale med den dataansvarlige og på dennes vegne.	Ingen bemærkninger.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførsel af sårbarhedsscanninger og penetrationstests. Inspiceret ved stikprøver, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger. Inspiceret, at evt. afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret samt meddelt de dataansvarlige i behørigt omfang.	Ingen bemærkninger
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Inspiceret ved udtræk af tekniske sikkerhedsparametre og -opsætninger, at systemer, databaser og netværk er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.	Ingen bemærkninger

Kontrolmål, kontrolaktivitet, test og resultat heraf

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Inspiceret ved en stikprøve på 1 medarbejderes adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov. Inspiceret ved en stikprøve på 1 fratrådt medarbejdere, at disses adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Inspiceret, at der foreligger dokumentation for regelmæssig - mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.	Ingen bemærkninger
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor autentifikation.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at to-faktor autentifikation anvendes ved behandling af personoplysninger, der medfører højrisiko for de registrerede. Inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører høj-risiko for de registrerede, alene kan ske ved anvendelse af to-faktor autentifikation.	Ingen bemærkninger
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Inspiceret dokumentation for, at kun autoriserede personer har haft fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger, i erklæringsperioden.	Ingen bemærkning

Kontrolmål, kontrolaktivitet, test og resultat heraf

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Ingen bemærkninger
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Inspiceret ved en stikprøve på 7 databehandleraftaler, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Ingen bemærkninger
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbeviser	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Inspiceret ved en stikprøve på 7 databehandleraftaler, at kravene til efterprøvning af medarbejdere i aftalerne er dækket af databehandlerens procedurer for efterprøvning. Inspiceret ved en stikprøve på 1 nyansatte medarbejdere i erklæringsperioden, at der er dokumentation for, at efterprøvningen har omfattet: · Referencer fra tidligere ansættelser · Straffeattest · Eksamensbeviser	Ingen bemærkninger

Kontrolmål, kontrolaktivitet, test og resultat heraf

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	Inspiceret ved en stikprøve på 1 nyansat medarbejder i erklæringsperioden, at de pågældende medarbejdere har underskrevet en fortrolighedsaftale. Inspiceret ved en stikprøve på 1 nyansat medarbejder i erklæringsperioden, at de pågældende medarbejdere er blevet introduceret til: · Informationssikkerhedspolitikken · Procedurer vedrørende databehandling, samt anden relevant information	Ingen bemærkninger
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages Inspiceret ved en stikprøve på 2 fratrådte medarbejdere i erklæringsperioden, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.	Ingen bemærkninger
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Inspiceret ved en stikprøve på 1 fratrådt medarbejdere i erklæringsperioden, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt.	Ingen bemærkninger
C.7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.	Ingen bemærkninger

Kontrolmål, kontrolaktivitet, test og resultat heraf

Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Inspiceret, at procedurerne er opdateret.	Ingen bemærkninger
D.2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: • Med mindre andet er angivet følger Bellcom de samme rutiner som for opbevaring af logs. Dvs man beholder data i 180 dage efter aftalens ophør. Så logs stadig er tilgængelige. • 180 dage efter ophør af databehandler aftalen er der kontrol af at data er slette. En bekræftelse af sletningen sendes til den data ansvarlige	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. OK Inspiceret ved en stikprøve på 7 databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder. Inspiceret ved en stikprøve på 7 databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger er slettet i overensstemmelse med de aftalte sletterutiner.	Ingen bemærkninger
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. OK Inspiceret ved en stikprøve på 1 ophørte databehandlinger i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	Ingen bemærkninger

Kontrolmål, kontrolaktivitet, test og resultat heraf

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Inspiceret, at procedurerne er opdateret. Inspiceret ved en stikprøve på 6 databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Ingen bemærkninger
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Inspiceret ved en stikprøve på 3 databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Ingen bemærkninger

Kontrolmål, kontrolaktivitet, test og resultat heraf

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Ingen bemærkninger
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Inspiceret ved en stikprøve på 1 underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Ingen bemærkninger
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	Ingen bemærkninger
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Inspiceret ved en stikprøve på 1 underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen bemærkninger

Kontrolmål, kontrolaktivitet, test og resultat heraf

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen bemærkninger
F.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende. Inspiceret dokumentation for, at information om opfølgning hos underdatabehandlere meddeles den dataansvarlige, således at denne kan tilrettelægge eventuelt tilsyn.	Ingen bemærkninger

Kontrolmål, kontrolaktivitet, test og resultat heraf

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at personoplysninger alene overføres til tredjelande eller internationale organisationer i henhold til aftale med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Inspiceret, at procedurerne er opdateret.	Ingen bemærkninger
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer. Inspiceret ved en stikprøve på dataoverførsler fra databehandlerens oversigt over overførsler, at der er dokumentation for, at overførslen er aftalt med den dataansvarlige i databehandleraftalen eller senere godkendt.	Ingen bemærkninger
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Inspiceret, at der foreligger formaliserede procedurer for sikring af et gyldigt overførselsgrundlag. Inspiceret, at procedurerne er opdateret. Inspiceret ved en stikprøve på dataoverførsel fra databehandlerens oversigt over overførsler, at der er dokumentation for et gyldigt overførselsgrundlag i databehandleraftalen med den dataansvarlige, samt at der kun er sket overførsler, i det omfang dette er aftalt med den dataansvarlige.	Ingen bemærkninger

Kontrolmål, kontrolaktivitet, test og resultat heraf

Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.	Ingen bemærkninger
H.2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: · Udlevering af oplysninger · Rettelse af oplysninger · Sletning af oplysninger · Begrænsning af behandling af personoplysninger · Oplysning om behandling af personoplysninger til den registrerede. Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.	Ingen bemærkninger

Kontrolmål, kontrolaktivitet, test og resultat heraf

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at proceduren er opdateret.	Ingen bemærkninger
I.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejdere • Overvågning af netværkstrafik • Opfølgning på logning af tilgang til personoplysninger	Inspiceret, at databehandler udbyder awareness- træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Inspiceret dokumentation for, at netværkstrafik overvåges, samt at der sker opfølgning på anormaliteter, overvågningsalarmer, overførsel af store filer mv. Inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang.	Ingen bemærkninger

Kontrolmål, kontrolaktivitet, test og resultat heraf

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 72 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Forespurgt underdatabehandlerne, om de har konstateret nogen brud på persondatasikkerheden i erklæringsperioden Inspiceret, at databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser. Inspiceret, at samtlige registrerede brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødig forsinkelse og senest 72 timer efter, at databehandleren er blevet opmærksom på brud på persondatasikkerheden.	Ingen bemærkninger
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for: · Beskrivelse af karakteren af bruddet på persondatasikkerheden · Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden · Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden. *ELLER HVIS BRUD I PERIODEN* Inspiceret dokumentation for, at der ved brud på persondatasikkerheden er truffet foranstaltninger, som har håndteret bruddet på persondatasikkerheden.	Ingen bemærkninger

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Palle Lysbjerg Hansen
Registreret revisor
Serienummer: 6a99e4f2-6dad-4bcc-a2dc-bfa8b3fa8210
IP: 212.130.xxx.xxx
2024-12-20 14:13:00 UTC

Linda Skov
Underskriver
Serienummer: 088751f7-2414-4438-ae5f-9f27cb202cf3
IP: 80.196.xxx.xxx
2024-12-20 14:21:00 UTC

Navnet er skjult
Underskriver
Serienummer: 8fc5cc07-65f9-442f-ae04-a819b9539a72
IP: 130.185.xxx.xxx
2024-12-20 15:56:13 UTC