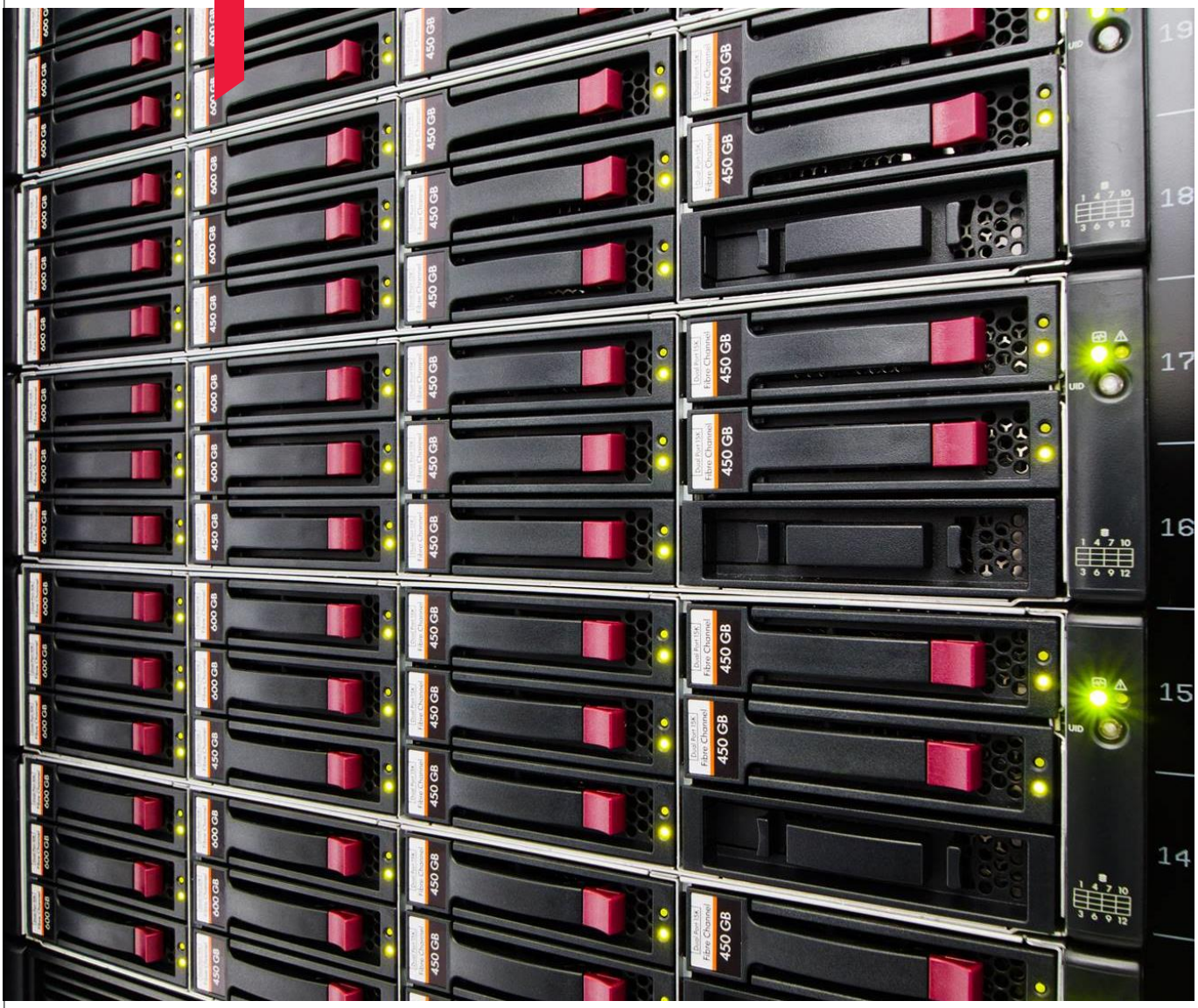


# BELLCOM HOSTING APS

## AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 19. DECEMBER 2019 OM BESKRIVELSEN AF OS2DAGSORDEN OG VALG-HALLA OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFOR-ANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

# INDHOLD

# UAFHÆNGIG REVISORS ERKLÆRING

## UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 19. DECEMBER 2019 OM BESKRIVELSEN AF OS2DAGSORDEN OG VALGHALLA OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

Til: Ledelsen i Bellcom Hosting ApS
Bellcom Hosting ApS kunder (dataansvarlige)

### Omfang

Vi har fået som opgave at afgive erklæring om den af Bellcom Hosting ApS (databehandleren) pr. 19. december 2019 udarbejdede beskrivelse på side 6 til 13 af OS2DAGSORDEN og VALGHALLA og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelse af personoplysninger i henhold til Europa-Parlaments og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) og lov om supplerende bestemmelser til databeskyttelsesforordningen (databeskyttelsesloven), og om udformningen af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vi har ikke udført handlinger vedrørende den operationelle effektivitet af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

### Databehandlerens ansvar

Databehandleren er ansvarlig for udarbejdelse af udtalelsen på side 4 og den medfølgende beskrivelse, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå udtalelsen og beskrivelsen er præsenteret. Databehandleren er endvidere ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, ligesom databehandleren er ansvarlig for at anføre kontrolmålene samt udforme og implementere kontroller for at opnå de anførte kontrolmål.

### Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i overensstemmelse med de internationale etiske regler for revisorer (IESBA's Etiske regler), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

Vi er underlagt den internationale standard om kvalitetsstyring ISQC 1, og vi anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

### Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om databehandlerens beskrivelse samt om udformningen af kontroller, der knytter sig til de kontrolmål, som er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse samt for kontrollernes udformning. De valgte handlinger afhænger af databehandlerens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte kontrolmål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet på side 4.

Som nævnt ovenfor har vi ikke udført handlinger vedrørende den operationelle effektivitet af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

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

**Begrænsninger i kontroller hos en databehandler**

Databehandlerens beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved anvendelsen af OS2DAGSORDEN og VALGHALLA, som hver enkelt dataansvarlig måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden.

**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 databehandlerens udtalelse på side 4. Det er vores opfattelse:

a. at beskrivelsen af OS2DAGSORDEN og VALGHALLA og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelses af personoplysninger i henhold til databeskyttelsesforordningen og databeskyttelsesloven, således som de var udformet og implementeret pr. 19. december 2019, i alle væsentlige henseender er retvisende, og

b. at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 19. december 2019.

**Beskrivelse af test af kontroller**

De specifikke kontroller, der blev testet, og resultater af disse tests fremgår på side 16 til 36.

**Tiltænkte brugere og formål**

Denne erklæring er udelukkende tiltænkt dataansvarlige, der har anvendt databehandlerens OS2DAGSORDEN og VALGHALLA, og som har en tilstrækkelig forståelse til at vurdere den sammen med anden information, herunder de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

København, den 8. januar 2020

**BDO Statsautoriseret revisionsaktieselskab**

Claus Bonde Hansen
Statsautoriseret revisor

Brian Bomholdt
Partner, CISA, CISM CISSP

## BELLCOM HOSTING APS' UDTALELSE

Bellcom Hosting ApS varetager behandling af personoplysninger i forbindelse med OS2DAGSORDEN og VALGHALLA for vores kunder, der er dataansvarlige i henhold til Europa-Parlaments og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) og lov om supplerende bestemmelser til databeskyttelsesforordningen (databeskyttelsesloven).

Medfølgende beskrivelse er udarbejdet til brug for de dataansvarlige, der har anvendt OS2DAGSORDEN og VALGHALLA, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

Bellcom Hosting ApS anvender en underdatabehandler. Denne underdatabehandlers relevante kontrolmål og tilknyttede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller indgår ikke i den medfølgende beskrivelse.

Bellcom Hosting ApS bekræfter, at den medfølgende beskrivelse på side 6 til 13 giver en retvisende beskrivelse af OS2DAGSORDEN og VALGHALLA og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller pr. 19. december 2019. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for OS2DAGSORDEN og VALGHALLA og hvordan de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller var udformet og implementeret, herunder redegør for:
    - De typer af ydelser der er leveret, herunder typen af behandlede personoplysninger.
    - De processer i både it-systemer og forretningsgange der er anvendt til at behandle personoplysninger og, om nødvendigt, at korrigere og slette personoplysninger samt at begrænse behandling af personoplysninger.
    - De processer der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige.
    - De processer der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.
    - De processer der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne.
    - De processer der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underretning til de registrerede.
    - De processer der sikrer passende tekniske og organisatoriske sikkerhedsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.
    - De kontroller, som med henvisning til afgrænsningen af OS2DAGSORDEN og VALGHALLA har forudsat ville være udformet og implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå kontrolmålene, er identificeret i beskrivelsen.

- De andre aspekter ved kontrolmiljøet, risikovurderingsprocessen, informationssystemerne og kommunikationen, kontrolaktiviteterne og overvågningskontrollerne, som har været relevante for behandlingen af personoplysninger.

2. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af OS2DAGSORDEN og VALGHALLA og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller under hensyntagen til, at denne beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved OS2DAGSORDEN og VALGHALLA, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

Bellcom Hosting ApS bekræfter, at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. 19. december 2019. Kriterierne anvendt for at give denne udtalelse var, at:

1. De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret.

2. De identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål.

Bellcom Hosting ApS bekræfter, at der er implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

Kolding, den 31. december 2019

**Bellcom Hosting ApS**

Jørn Skifter Andersen
Partner

# BELLCOM HOSTING APS' BESKRIVELSE AF OS2DAGSORDEN OG VALGHALLA

## Bellcom Hosting ApS

Bellcom er en 100 % danskejet virksomhed, der siden 1991 har specialiseret sig i effektive IT-løsninger for alle typer kunder, små som store.

Bellcom ejer i dag et komplet server hosting miljø som supporterer vore kunder. Dette er opstillet i et professionelt og sikkert datacenter med alt hvad dertil hører af overvågning, strømbackup og brandslukning. Systemet er opbygget på en sådan måde, at det hurtigt og nemt kan 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 supportafdelingen. IT-drift har ansvaret for drift, vedligeholdelse og videreudvikling af vores hostingmiljø. Ledelsen hos Bellcom har det overordnede ansvar for IT-sikkerheden i virksomheden.

## OS2DAGSORDEN og VALGHALLA og behandling af personoplysninger

**Behandling af personoplysninger**
For OS2DAGSORDEN behandles udelukkende almindelige personoplysninger vedr. administrativt personale og øvrigt servicepersonale hos kunden.
For VALGHALLA 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.

**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 pc'er 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-, formandskabs- 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 får evnen til at gennemse historiske møder og en samlet orientering om aktuelle og udvalgte mødeaktiviteter, alt efter den pågældende brugers rolle og/eller rettigheder.

OS2DAGSORDEN giver derudover 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 følsomme persondata. I løsningen er der indbygget logning af adgangen til alle data i henhold til retningslinjerne fra Datatilsynet.

**Platformen VALGHALLA**
Der skal mange ting til for at få et valg til at køre som smurt. Her kommer VALGHALLA ind i billedet.

VALGHALLA 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 VALGHALLA, og de kan brug VALGHALLA til at kommunikere med valgsekretariatet.

VALGHALLA 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.

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

Platformen VALGHALLA indeholder blandt andet CPR-numre. I løsningen er der indbygget logning af adgangen til alle data i henhold til retningslinjerne fra Datatilsynet. Løsningen er under videreudvikling og splittes snart op i en ekstern og intern serveropsætning, hvorved der alene udstilles data til brug for planlægningen findes på den offentlige server. Og alle persondata forbliver på den interne server.

## Sikkerhedsopdateringer

I Bellcom har vi sat sikkerhedsopdateringerne i system. For følsomme personoplysninger 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 sårbart 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

## Styring af persondatasikkerhed

Bellcom har opstillet krav til etablering, implementering, vedligeholdelse og løbende forbedring af et ledelsessystem for persondatasikkerhed, der sikrer opfyldelse af indgåede aftaler med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

De tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller til beskyttelse af personoplysninger er udformet i henhold til risikovurderinger og implementeres for at sikre fortrolighed, integritet og tilgængelighed samt overholdelse af den gældende databeskyttelseslovgivning. Sikkerhedsforanstaltninger og kontroller er i videst muligt omfang automatiserede og teknisk understøttet af it-systemer.

Styringen af persondatasikkerheden samt de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller er struktureret i følgende hovedområder, for hvilke der er defineret kontrolmål og kontrolaktiviteter:

| ARTIKEL | OMRÅDE |
|---|---|
| Artikel 28, stk. 1 | Databehandlerens garantier |

| ARTIKEL | OMRÅDE |
|---|---|
| Artikel 28, stk. 3 | Databehandleraftale |
| Artikel 28, stk. 3, litra a og h, og stk. 10<br>Artikel 29<br>Artikel 32, stk. 4 | Instruks for behandling af personoplysninger |
| Artikel 28, stk. 2 og 4 | Underdatabehandlere |
| Artikel 28. stk. 3, litra b | Fortrolighed og lovbestemt tavshedspligt |
| Artikel 28, stk. 3, litra c | Tekniske og organisatoriske sikkerhedsforanstaltninger |
| Artikel 25 | Databeskyttelse gennem design og standardindstillinger. |
| Artikel 28, stk. 3, litra g | Sletning og tilbagelevering af personoplysninger |
| Artikel 28, stk. 3, litra e, f og h | Bistand til den dataansvarlige |
| Artikel 30, stk. 2, 3 og 4 | Fortegnelse over kategorier af behandlingsaktiviteter |
| Artikel 33, stk. 2 | Underretning om brud på persondatasikkerheden. |

## 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 revision 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 en underleverandør i forbindelse med opbevaring af en kopi af den samlede backup. Der stilles krav om, at denne underleverandører besidder et ISO/IEC 27001:2013 certifikat samt undergår uafhængig revision.

## 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.

**Risikostyring i Bellcom**
Vi har procedurer for løbende risikovurdering af vores forretning og specielt vores hosting-ydelse. 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 sikkerhedshåndtering samt kodeordsskift 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 Bellcoms ledelse.

**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 opdateringsaftaler, 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 tredjeparter, 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.

**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.

**Underleverandører**
Hvor vi bruger underleverandører fører vi tilsyn med disse. Bellcom benytter overvejende ikke underleverandører.

**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.

**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.

Serverrum
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.

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 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.

Adgangen sker via storrumskontor således, at uvedkommende ikke uautoriserede 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.

**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 supportsystem samt vores projektplanlægningsværktøjer.

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.

**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 igennem 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.

**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 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 til vores co-location ved hjælp af vores backup-system. Dermed er data fysisk separeret fra vores driftssystemer, og efter endt afvikling foretages der en automatiseret verificering af, hvorvidt datamængde og indhold mellem vores driftssystem og colocation, stemmer overens.

En ansvarlig medarbejder sikrer herefter, at sikkerhedskopieringen er sket, foretager det fornødne hvis jobbet er fejlet, og logfører herefter dette.

**Bortskaffelse**
Alt databærende udstyr destrueres inden bortskaffelse, for at sikre, at data ikke er tilgængeligt.

**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 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.

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.

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 påvirkninger (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.

**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 fallback-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.

Planen og procedurerne er forankret i vores driftsdokumentation og procedurer.

**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
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)

Informationssikkerhedsbrud
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 e-mail 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.

## 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, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST

## Formål og omfang

BDO har udført sit arbejde i overensstemmelse med ISAE 3000 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger.

BDO har udført handlinger for at opnå bevis for oplysningerne i Bellcom Hosting ApS beskrivelse af OS2-DAGSORDEN og VALGHALLA samt for udformningen af de tilhørende tekniske og organisatoriske sikkerheds-foranstaltninger og øvrige kontroller. De valgte handlinger afhænger af BDO's vurdering, herunder vurde-ringen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt ud-formet.

BDO's test af udformningen af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller samt implementeringen heraf har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af Bellcom Hosting ApS og som fremgår af efterfølgende kontrolskema.

I kontrolskemaet har BDO beskrevet de udførte test, der blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og at de tilhørende kontroller var hen-sigtsmæssigt udformet pr. 19. december 2019.

## Udførte testhandlinger

Test af udformningen af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller samt implementeringen heraf er udført ved forespørgsel, inspektion og observation.

| Type | Beskrivelse |
|---|---|
| Forespørgsel | Forespørgsler hos passende personale er udført for alle væsentlige kontrolaktiviteter.<br><br>Forespørgslerne blev udført for blandt andet at opnå viden og yderligere oplysninger om ind-førte politikker og procedurer, herunder hvordan kontrolaktiviteterne udføres, samt at få be-kræftet beviser for politikker, procedurer og kontroller. |
| Inspektion | Dokumenter og rapporter, der indeholder angivelse om udførelse af kontrollen, er gennemlæ-ste med det formål at vurdere udformningen og overvågningen af de specifikke kontroller, herunder om kontrollerne er udformede, således at de kan forventes at blive effektive, hvis de implementeres, og om kontrollerne overvåges og kontrolleres tilstrækkeligt og med pas-sende intervaller.<br><br>Test af væsentlige systemopsætninger af tekniske platforme, databaser og netværksudstyr er udført for at påse, om kontroller er implementerede, herunder eksempelvis vurdering af log-ning, sikkerhedskopiering, patch management, autorisationer og adgangskontroller, data-transmission samt besigtigelse af udstyr og lokaliteter. |
| Observation | Anvendelsen og eksistensen af specifikke kontroller er observeret, herunder test for at påse, at kontrollen er implementeret. |

For de ydelser, som Hetzner Online GmbH leverer inden for hosting og drift af it, har vi modtaget revisi-onsrapport fra TÜVRheinland pr. 25. januar 2019 for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

Denne underdatabehandlers relevante kontrolmål og tilknyttede kontroller indgår ikke i Bellcom Hosting ApS' beskrivelse af OS2DAGSORDEN og VALGHALLA og de tilhørende tekniske og organisatoriske sikker-hedsforanstaltninger og øvrige kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos Bellcom Hosting ApS, der sikrer udførelsen af et behørigt tilsyn med underdatabe-handlerens opfyldelse af den mellem underdatabehandleren og databehandleren indgåede databehandler-aftale og opfyldelse af databeskyttelsesforordningen og databeskyttelsesloven.

**Resultat af test**

Resultatet af de udførte test af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller angiver, om den beskrevne test har givet anledning til at konstatere afvigelser.

En afvigelse foreligger, når:

- Tekniske eller organisatoriske sikkerhedsforanstaltninger eller øvrige kontroller mangler at blive udformet og implementeret for at kunne opfylde et kontrolmål.
- Tekniske eller organisatoriske sikkerhedsforanstaltninger eller øvrige kontroller, der knytter sig til et kontrolmål, ikke er hensigtsmæssigt udformet eller implementeret.

## Artikel 28, stk. 1: Databehandlerens garantier

**Kontrolmål**

- *At sikre, at databehandleren kan stille de fornødne garantier til beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og beskyttelsen af den registreredes rettigheder.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Informationssikkerhedspolitik**<br><br>▶ Politikker for informationssikkerhed er fastlagt af Bellcoms ledelse.<br>▶ Bellcom har udarbejdet og implementeret procedurer og politik for behandling af persondata.<br>▶ Bellcoms procedurer og politikker angående personoplysninger bliver gennemgået og opdateret minimum en gang årligt. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspicereret politik for behandling af persondata og observeret, at den er godkendt 25. oktober 2019.<br><br>Vi har stikprøvevis udvalgt en medarbejder og observeret, at medarbejderen er orienteret om håndtering af persondata.<br><br>Vi har inspiceret årshjul og observeret, at politikker og procedurer skal gennemgås minimum én gang om året. | Ingen afvigelser konstateret. |
| **Gennemgang af informationssikkerhedspolitik**<br><br>▶ Bellcom foretager en årlig revidering og opdatering af informationssikkerhedspolitikker.<br>▶ Bellcom laver årlig intern revidering af gennemførte kontroller. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret it-sikkerhedspolitikken og observeret, at denne er godkendt af Bellcoms ledelse den 16. oktober 2019.<br><br>Vi har inspicereret Bellcoms årshjul og observeret, at der skal foretages en revision i 2020. | Ingen afvigelser konstateret. |
| **Organisering af informationssikkerhedspolitik**<br><br>▶ Informationssikkerhedspolitikker er kommunikeret til alle medarbejdere.<br>▶ Alle medarbejdere i Bellcom er bekendte med deres roller og ansvar.<br>▶ Alle underleverandører og tredjeparter er bekendte med deres roller og ansvar.<br>▶ Alle medarbejdere og kontrahenter er kvalificerede og egnede til at udføre deres rolle. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har ved interview af en tilfældigt udvalgt medarbejder fået bekræftet, at medarbejdere er informeret om it-sikkerhedspolitikken.<br><br>Vi har udtaget og inspiceret en stikprøve for test af kontrollen. Vi har observeret, at medarbejderen har underskrevet erklæring om overholdelse af it-sikkerhedspolitikken. | Ingen afvigelser konstateret. |

| **Kontrolmål**<br>▶ *At sikre, at databehandleren kan stille de fornødne garantier til beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og beskyttelsen af den registreredes rettigheder.* | | |
|---|---|---|
| **Kontrolaktivitet** | **Test udført af BDO** | **Resultat af test** |
| ▶ Rolle- og ansvarsbeskrivelsen, herunder opgaver og ansvar i forhold til sikkerheden, er defineret i de udarbejdede rollebeskrivelser, medarbejdernes ansættelseskontrakt samt i IT-sikkerhedspolitikken.<br>▶ Ansvar for IT-drift, Udvikling og support er fastlagt af ledelsen.<br>▶ Bellcom har udformet og implementeret procedurer for ansættelse af medarbejdere og etablering af samarbejde med eksterne kontrahenter. | Vi har inspicereret en stikprøve af ansættelseskontrakter og observeret, at medarbejderens rolle er beskrevet.<br><br>Vi har inspicereret organisationsdiagram samt beskrivelser og observeret, at ansvaret for it er fastlagt.<br><br>Vi har inspicereret procedure og observeret, at Bellcom har definereret procedure for ansættelse af medarbejder. | |
| **Rekruttering af medarbejdere**<br><br>▶ Bellcom har en procedure for kompetencetjek af potentielle medarbejdere før ansættelse. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspicereret kompetencetjek af medarbejder inden ansættelsen og observeret, at uddannelsesaftale og straffeattest er blevet indhentet. | Ingen afvigelser konstateret. |
| **Awareness og oplysningskampagner for medarbejdere**<br><br>▶ Bellcom holder medarbejderne informeret om procedurer og politikker angående behandling af personoplysninger. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har stikprøvevis udvalgt udsendt nyhedsbrev og observeret, at medarbejderne orienteres om behandling af personoplysninger. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3: Databehandleraftale

**Kontrolmål**

- *At sikre, at databehandleren indgår en skriftlig kontrakt med den dataansvarlige, der fastsætter vilkårene for behandlingen af den dataansvarliges personoplysninger, og at kontrakten opbevares elektronisk.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Indgåelse af databehandleraftale med den dataansvarlige**<br><br>▶ Bellcom har indgået databehandleraftale med dataansvarlige, ved brug af udarbejdet standarddatabehandleraftale.<br>▶ Der er implementeret procedurer for indhentelse og vurdering af databehandleraftale med dataansvarlig.<br>▶ Bellcom har procedure for databehandleraftaler er underskrevet af begge parter.<br>▶ Bellcom opbevarer databehandleraftalerne elektronisk. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspicereret skabeloner for databehandleraftaler og observeret, at skabelonerne er opdateret med relevant informationer.<br><br>Vi har inspicereret procedure og observeret, at databehandleraftaler med dataansvarlig skal vurderes og indhentes.<br><br>Vi har stikprøvevis udvalgt databehandleraftale og observeret, at databehandleraftalen med dataansvarlig ikke er underskrevet af dataansvarlig. Vi har observeret, at der forelægger en proces for indgåelse af databehandleraftale.<br><br>Vi har inspicereret digital oversigt over databehandleraftaler og observeret, at aftalerne opbevares elektronisk. | Vi har via vores stikprøve konstateret, at Bellcom er i gang med at indgå databehandleraftale med en dataansvarlig. Processen for indgåelse af aftaler er igangværende for de kunder, der mangler.<br><br>Ingen yderligere afvigelser konstateret. |
| **Styring af underdatabehandlere**<br><br>▶ Bellcom har en procedure for, at indgåede databehandleraftaler indeholder brugen af underdatabehandlere. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har stikprøvevis udvalgt en databehandleraftale og observeret, at underdatabehandleren fremgår i databehandleraftalen. | Ingen afvigelser konstateret. |

| Artikel 28, stk. 3 og 10, artikel 29 og artikel 32, stk. 4: Instruks for behandling af personoplysninger | | |
|---|---|---|
| **Kontrolmål**<br>▶ *At sikre, at databehandleren alene handler efter dokumenteret instruks fra den dataansvarlige.*<br>▶ *At sikre, at databehandleren underretter den dataansvarlige, hvis en instruks er i strid med databeskyttelsesforordningen og databeskyttelsesloven.* | | |
| **Kontrolaktivitet** | **Test udført af BDO** | **Resultat af test** |
| **Instruks for behandling af personoplysninger**<br><br>▶ Bellcom har procedurer for udarbejdelse af databehandleraftale, herunder indhentning af instruks fra den dataansvarlige eller samarbejde om udarbejdelse af instruks i medfør af databehandleraftalen.<br>▶ Bellcom behandler persondata efter instruks fra dataansvarlig. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret proceduren for udarbejdelse af databehandleraftale og observeret, at instruks skal indhentes fra den dataansvarlige.<br><br>Vi har stikprøvevis udvalgt databehandleraftale og observeret, at der er indhentet instruks fra den dataansvarlige. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 2 og 4: Underdatabehandlere

**Kontrolmål**

- *At sikre, at underdatabehandleren er pålagt de samme databeskyttelsesforpligtelser, som databehandleren er pålagt af den dataansvarlige, ved indgåelse af en skriftlig kontrakt med tilhørende instruks.*
- *At sikre, at den dataansvarlige har givet en forudgående specifik eller generel skriftlig godkendelse af underdatabehandlere.*
- *At sikre, at underdatabehandleren kan stille de fornødne garantier til beskyttelse af personoplysningerne i overensstemmelse med kontrakten.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Underdatabehandleraftale og instruks**<br><br>▶ Bellcom har indgået underdatabehandleraftaler med underdatabehandlere.<br>▶ Underdatabehandlere er pålagt samme databeskyttelsesforpligtelser som databehandler er pålagt af de dataansvarlige. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret underdatabehandleraftale og observeret, om underdatabehandleraftalen med Hetzner Online GmbH Gunzenhausen er omfattet af samme databeskyttelsesforpligtelser som Bellcom er underlagt. | Vi har konstateret, at der ikke foreligger en dokumenteret sammenholdelse af kravene, i Bellcoms databehandleraftaler med kunderne, med Bellcoms databehandleraftale med underdatabehandleren.<br><br>Ingen yderligere afvigelser konstateret. |
| **Godkendelse af underdatabehandlere**<br><br>▶ Dataansvarlige har givet skriftlig godkendelse af underdatabehandlere. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har for en tilfældigt udvalgt stikprøve inspiceret databehandleraftale og observeret, at der er givet specifik godkendelse af Bellcoms anvendelse af underdatabehandlere. | Ingen afvigelser konstateret. |
| **Tilsyn med underdatabehandlere**<br><br>▶ Bellcom indhenter og vurderer revisorerklæring, ISO 27001 certificering eller lignende dokumentation for underdatabehandlere. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret politikker og procedure og observeret, at Bellcom skal indhente og vurdere revisorerklæringer.<br><br>Vi har ved interview med medarbejder fået bekræftet medarbejderens forståelse for indhentelse af revisorerklæring fra underdatabehandlere og gennemgang af disse.<br><br>Vi har observeret, at der er indhentet ISO 27000-certifikat for Hetzner Online GmbH. Vi har ligeledes inspiceret revisionsrapport for Hetnzner Online GmbH og observeret der ikke er bemærkninger. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra b: Fortrolighed og lovbestemt tavshedspligt

**Kontrolmål**

- *At sikre, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Tavsheds- og fortrolighedsaftale med medarbejdere**<br><br>▶ Alle medarbejdere i Bellcom er underlagt vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, som er beskrevet i ansættelseskontrakten. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret procedure for baggrundscheck og observeret, at der skal underskrives ansættelseskontrakt med tilhørende tavshedserklæring.<br><br>Vi har for en tilfældigt udvalgt stikprøve observeret, at tavshedserklæringen er underskrevet ved ansættelse. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**Kontrolmål**

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Risikovurdering**<br><br>▶ Bellcom foretager en risikovurdering af selskabets informationsaktiver og systemer med afsæt i den registreredes rettigheder. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspicereret risikovurdering og observeret, at der er foretaget en risikovurdering af den fysiske og logiske sikkerhed i forhold til driftssikkerhed og tilgængelighed. | Vi har konstateret, at der ikke er foretaget en formel risikovurdering af de registreres rettigheder.<br><br>Ingen yderligere afvigelser konstateret. |
| **Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse**<br><br>▶ Bellcom har udarbejdet en overordnet beredskabsplan for reetablering af drift.<br>▶ Beredskabsplanen afprøves og vedligeholdes 1 gang årligt. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret beredskabsplan for Bellcoms it-drift og observeret, at beredskabsplanen omfatter organisering, instruktion til systemgendannelse og kontakt til leverandører.<br><br>Vi har inspicereret beredskabsplanen og observeret, at den er opdateret pr. 9. november 2019.<br><br>Vi har inspicereret plan for test af beredskabsplan og observeret, at denne testes den 13. december 2019, men ikke er testet. | Vi har konstateret, at beredskabsplanen ikke er afprøvet.<br><br>Ingen yderligere afvigelser konstateret. |
| **Håndtering af inddata- og uddatamaterialer**<br><br>▶ Opbevaring eller håndtering af kundedata på flytbare medier sker kun med forudgående skriftlig aftale med dataansvarlig. | Vi har udført forespørgsler hos passende personale. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**Kontrolmål**

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| | Vi har inspicereret politik og procedurer og observereret, at Bellcom opbevarer og håndterer kundedata på stationære medier.<br><br>Vi har ikke kunnet efterprøve disse procedurer, da der ikke har været opbevaring eller håndtering af kundedata på flytbare medier. | |
| **Fysisk adgangskontrol**<br><br>- Indgangsdør til kontor er aflåst hvis der ikke er bemanding i kontor.<br>- Kontoret er sikret med tyverialarm. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har ved inspektion af de fysiske lokaler observeret, at indgangsdøren er aflåst ved ankomst.<br><br>Vi har inspiceret liste over medarbejdere med nøglechip til kontoret og observeret, at kontoret er beskyttet med alarm. | Ingen afvigelser konstateret. |
| **Sikring af udstyr og aktiver**<br><br>- Flytbare medier beskyttes mod miljømæssige påvirkninger samt hærværk og tyveri. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspicereret procedure og observeret, at flytbare medier bliver beskyttet i datacenter og kontor. | Ingen afvigelser konstateret. |
| **Fysisk sikkerhed i datacenter** | Vi har udført forespørgsler hos passende personale. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**Kontrolmål**

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| ▶ Servere, services, data og informationer er afskærmet mod miljømæssige påvirkninger (brand, vand, temperatur mv.)<br>▶ Servere, services, data og informationer er sikret mod hærværk, tyveri mv<br>▶ Adgang til datacenter sker med nøgle udenfor åbningstid<br>▶ Adgang til forrummet og datacenter sker med brik og nøgle.<br>▶ Uautoriseret adgang, uden brug af brik, giver alarm til Dansikring.<br>▶ Serverrummet er klima- og brandbeskyttet<br>▶ Autoriseret adgang til serverrum udløser SMS til driftsleder og driftsteam, og der sker fotodokumentation af, hvem der er i rummet.<br>▶ Serverrummet er forsynet med CTS-kontrolsystem (teknik- og miljøvagt).<br>▶ Alle systemer og sensorer overvåges af CTS, og overvågningsdata logges.<br>▶ Servere er beskyttet mod strømsvigt via UPS og generator. | Vi har ved inspektion i hosting-centret observeret, at servere er beskyttet med nødstrøm, køling og brandslukningsudstyr.<br><br>Vi har inspiceret kontrakter og servicerapporter for brandsikring, overvågning, køleanlæg, nødstrømsgenerator og tyverialarm. Vi har observeret, at der forefindes underskrevne tjeklister for kvartalsvise kontroller af hosting-centret.<br><br>Vi har observeret, at adgang til hosting-centret sker med adgangskode og nøglechip. Vi har observeret, at der findes 2 nøglechips til hosting-centret, som er udleveret til databehandlerens ledelse.<br><br>Vi har fået oplyst, at ved behov for adgang til hosting-centret skal medarbejdere og serviceleverandører henvende sig til databehandlerens ledelse for udlevering af nøglechip.<br><br>Vi har observeret, at hosting-centret overvåges via CTS system, hvorved overvågningskamera automatisk aktiveres, når døren til rummet åbnes. Logning af adgang til hosting-centret opsamles i CTS-systemet.<br><br>Vi har observeret, at servere er beskyttet mod strømsvigt. | |
| **Logisk adgangskontrol**<br><br>▶ Bellcom har udformet procedurer for brugeradministration.<br>▶ Oprettelse af brugere godkendes af ledelsen. | Vi har udført forespørgsler hos passende personale. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**Kontrolmål**

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| ▶ Brugere gennemgås mindst én gang årligt.<br>▶ Systemadministratoradgang tildeles efter arbejdsbetinget behov.<br>▶ Password skal skiftes mindst hver 3. måned.<br>▶ Password skal leve op til krav for sikre password. | Vi har inspiceret procedure for brugeradministration og observeret, at der er udformet procedure for oprettelse og nedlæggelse af brugere i VALGHALLA og OS2DAGSORDEN.<br><br>Vi har inspiceret oprettelse af brugere og observeret, at der er tildelt adgang efter ledelsesgodkendelse.<br><br>Vi har inspiceret procedure for gennemgang af brugere og har observeret, at der er foretaget gennemgang af brugere i VALGHALLA den 5. december 2019.<br><br>Vi har observeret, at brugergennemgang i driftssystemer er foretaget den 5. december 2019.<br><br>Vi har inspiceret lister over brugere med privilegeret adgang og observeret, at dette er tildelt medarbejdere med et arbejdsbetinget behov.<br><br>Vi har inspiceret medarbejderinstruktion og observeret, at retningslinjer for krav til password, skift af password og anvendelse af password i applikationer er beskrevet.<br><br>Vi har observeret, at medarbejdere har underskrevet erklæring om, at de overholder politikker for logiske adgangskontroller. | |
| **Eksterne kommunikationsforbindelser**<br><br>▶ Kommunikation med dataansvarlige sker via e-mail eller projektplanlægningsværktøjer.<br>▶ Kommunikation er krypteret. | Vi har udført forespørgsler hos passende personale. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**Kontrolmål**

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| | Vi har inspiceret it-sikkerhedspolitikken og medarbejderinstruktionen og observeret, at der er udformet retningslinjer for håndtering af persondata og kommunikation.<br><br>Vi har inspiceret systemkonfiguration for kryptering af datakommunikation og observeret, at der anvendes kryptering ved kommunikation. | |
| **Firewall**<br><br>▶ Servere og data er beskyttet af firewall. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret datacenter og systemkonfiguration og observeret, at netværket er beskyttet af redundante firewalls. | Ingen afvigelser konstateret. |
| **Antivirusprogram**<br><br>▶ Servere og systemer er beskyttet af antivirus software. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret systemkonfiguration for antivirus og har observeret, at der er installeret antivirus software og scanning af mailsystem. | Ingen afvigelser konstateret. |
| **Sikkerhedskopiering og retablering af data**<br><br>▶ Der foretages sikkerhedskopiering af alle kritiske data og services.<br>▶ Der gennemføres kontrol og verificering af backup og systemgendannelse. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret procedurer for sikkerhedskopiering, verificering af backup og systemgendannelse. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**Kontrolmål**

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| ▶ Kontrol og test af sikkerhedskopiering dokumenteres i log.<br>▶ Backup kopieres til ekstern sikker lokation én gang i døgnet.<br>▶ Der gennemføres verificering af succesfuld kopiering til ekstern lokation efter hver kopiering.<br>▶ Procedurer for systemgendannelse er dokumenteret og afprøves løbende. | Vi har observeret, at ansvar for at gennemgang og verificering af den natlige sikkerhedskopiering er placeret.<br><br>Vi har observeret, at der er foretaget systemgendannelse.<br><br>Vi har inspiceret systemkonfiguration for sikkerhedskopiering og har observeret, at der er konfigureret daglig sikkerhedskopiering.<br><br>Vi har inspicereret udskrift af servicedesk-system og observeret, at daglig gennemgang er opsat som en daglig tilbagevendende opgave.<br><br>Vi har inspiceret udskrift fra backuplog for kontrol af sikkerhedskopiering og har observeret, at der er foretaget sikkerhedskopiering af servere. | |
| **Vedligeholdelse af systemsoftware**<br><br>▶ Der er udarbejdet systemdokumentation for driftskritiske systemer.<br>▶ Systemdokumentation opbevares på to af hinanden uafhængige lokationer. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspicereret beskrivelse af systemet og observeret, at der forelægger dokumentation af driftskritiske systemer.<br>Vi har inspicereret opbevaring af systemdokumentation og observeret, at de forelægger i et henholdsvis lukket og åbent miljø. | Ingen afvigelser konstateret. |
| **Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger** | | |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**Kontrolmål**

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| ▶ Drifts kritiske servere og udstyr overvåges.<br>▶ Der foretages daglig gennemgang af overvågning.<br>▶ Ved overskridelse af grænseværdier for overvågning, registreres der automatisk hændelse og alarmering sker via SMS. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret procedure for logning.<br><br>Vi har inspiceret system for logning og observeret, at der foretages logning på driftskritiske systemer. | Ingen afvigelser konstateret. |
| **Reparation og service samt bortskaffelse af it-udstyr**<br><br>▶ Alt databærende udstyr destrueres inden bortskaffelse. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret procedure for destruktion og har observeret, at der er udformet en procedure for fysisk destruktion af databærende medier.<br><br>Vi har ikke kunnet efterprøve disse procedurer, da der ikke har været bortskaffelse af udstyr i perioden. | Ingen afvigelser konstateret. |
| **Styring af hemmelig autentifikationsinformation om brugere**<br><br>▶ Udlevering af glemte kodeord, personoplysninger, bestillinger, sker opdelt via 2 forskellige kommunikationsplatforme, E-mail og SMS. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspicereret udlevering af glemt kodeord, og at dette foretages skriftligt på e-mail. | Ingen afvigelser konstateret. |
| **Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger**<br><br>▶ Alle sikkerhedsdokumenter, inklusiv detaljerede sikkerhedsforanstaltninger, er vurderet årligt. | Vi har udført forespørgsler hos passende personale. | Vi har konstateret, at Bellcom ikke formelt har vurderet og evalueret effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden. |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**Kontrolmål**

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| ▶ Hvis der sker ændringer i løbet af året, bliver foranstaltninger evalueret.<br>▶ Bellcom afprøver jævnligt sikkerhedsforanstaltningerne. | Vi har inspiceret it-sikkerhedspolitikken og observeret, at denne er godkendt af Bellcoms ledelse den 16. oktober 2019.<br><br>Vi har inspiceret stikprøvevis udvalgte procedurer, og observeret, at beredskabsplanen ikke er vurderet og evalueret efter informationssikkerhedsbrud. | Ingen yderligere afvigelser konstateret. |

| Artikel 25: Databeskyttelse gennem design og standardindstillinger | | |
|---|---|---|
| **Kontrolmål**<br>▶ *At sikre, at databehandleren gennemfører databeskyttelse gennem design og standardindstillinger.* | | |
| **Kontrolaktivitet** | **Test udført af BDO** | **Resultat af test** |
| **Udvikling og vedligeholdelse af systemer**<br>▶ Bellcom har udformet og implementeret procedure for ændringsstyring.<br>▶ Alle større eller forretningskritiske ændringer er underlagt procedure for ændringsstyring. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret procedure for ændringsstyring og har observeret, at den indeholder relevante områder.<br><br>Vi har stikprøvevis udvalgt en udført ændringsopgave og observeret, at proceduren er implementeret. | Ingen afvigelser konstateret |
| **Informationssikkerhed i udvikling og ændringer**<br>▶ Kildekode opbevares i et versionsstyringssystem der er tilgængeligt for kunderne. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret it-politikker og procedurer samt system for opbevaring af kildekode. Vi har observeret, at kildekode opbevares i GitHub og versionsstyres i denne. | Ingen afvigelser konstateret. |
| **Adskillelse af udviklings-, test og produktionsmiljø**<br>▶ Drift- og testmiljø er adskilt.<br>▶ Alle produkter og ændringer testes i testmiljø før der overføres ændringer til produktionsmiljø. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspicereret procedure for udvikling og observeret, at drift -og testmiljø skal være adskilt.<br><br>Vi har stikprøvevis udvalgt en ændringsopgave og observeret, at der er adskillelse mellem medarbejder, der udvikler og tester.<br><br>Vi har stikprøvevis udvalgt en kunde og observeret, at drift og testmiljø er adskilt. | Ingen afvigelser konstateret |

## Artikel 28, stk. 3, litra g: Sletning

**Kontrolmål**

- *At sikre, at databehandleren kan slette, efter at tjenesten vedrørende behandlingen er ophørt, i henhold til instruks fra den dataansvarlige.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Sletning af personoplysninger**<br><br>- Bellcom sletter data efter anmodning fra den dataansvarlige i henhold til indgået databehandleraftale.<br>- Bellcom har procedure for databehandleraftaler, indeholder informationer om slettefrister. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspicereret proceduren for sletning og observeret, at det kun er den dataansvarlige, der via systemet kan slette brugere.<br><br>Vi har inspicereret opsætningen i systemet og observeret, at den dataansvarlige kan slette personoplysninger.<br><br>Vi har inspiceret proceduren og observeret, at ved ophør af kunde skal personoplysninger slettes.<br><br>Vi har ikke kunnet efterprøve disse procedurer, da der ikke har været forespørgsler fra dataansvarlige om sletning. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra e, f og h: Bistand til den dataansvarlige

**Kontrolmål**

- *At sikre, at databehandleren kan bistå den dataansvarlige med opfyldelse af de registreredes rettigheder.*
- *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til behandlingssikkerhed (artikel 32), brud på persondatasikkerheden (artikel 33-34) og konsekvensanalyser (artikel 35-36).*
- *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til revision og inspektion.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **De registreredes rettigheder**<br><br>▶ Bellcom har procedurer for at kunne bistå den dataansvarlige med opfyldelse af de registreredes rettigheder.<br>▶ Bellcom har udarbejdet og implementeret procedurer for, at henvendelser fra registrerede videresendes til dataansvarlig. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret procedure for bistand til dataansvarlig og observeret, at Bellcom skal bistå dataansvarlig med opfyldelse af de registreredes rettigheder.<br><br>Vi har inspiceret databehandleraftale med den dataansvarlige og observeret, at bistand til den dataansvarlige i forhold til dennes forpligtelser overfor den registrerede er beskrevet.<br><br>Vi har ikke kunnet efterprøve disse procedurer, da der ikke har været forespørgsler fra dataansvarlige om bistand. | Ingen afvigelser konstateret. |
| **Forpligtelser om behandlingssikkerhed, brud på persondatasikkerheden og konsekvensanalyser**<br><br>▶ Bellcom har procedurer for at kunne bistå den dataansvarlige i forhold til overholdelse af særlige krav i forordningen, herunder bistand i forhold til artikel 32 – 36. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret procedure for bistand til dataansvarlig og observeret, at Bellcom vil bistå dataansvarlig ved særlige krav i forordningen.<br><br>Vi har ikke kunnet efterprøve disse procedurer, da der ikke har været forespørgsler fra dataansvarlige om bistand i forhold til artikel 32 – 36. | Ingen afvigelser konstateret. |

| Artikel 28, stk. 3, litra e, f og h: Bistand til den dataansvarlige | | |
|---|---|---|
| **Kontrolmål**<br>▶ *At sikre, at databehandleren kan bistå den dataansvarlige med opfyldelse af de registreredes rettigheder.*<br>▶ *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til behandlingssikkerhed (artikel 32), brud på persondatasikkerheden (artikel 33-34) og konsekvensanalyser (artikel 35-36).*<br>▶ *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til revision og inspektion.* | | |
| Kontrolaktivitet | Test udført af BDO | Resultat af test |
| **Revision og inspektion**<br><br>▶ Bellcom har procedurer for at kunne bistå den dataansvarlige i forhold til revision og inspektion. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspicereret proceduren for bistand til dataansvarlig og observeret, at Bellcom vil bistå dataansvarlig i forhold til revision og inspektion.<br><br>Vi har ikke kunnet efterprøve disse procedurer, da der ikke har været forespørgsler fra den dataansvarlige. | Ingen afvigelser konstateret. |

| Artikel 30, stk. 2, 3 og 4: Fortegnelse over kategorier af behandlingsaktiviteter | | |
|---|---|---|
| **Kontrolmål**<br>▶ *At sikre, at databehandleren udarbejder en skriftlig fortegnelse over alle kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige.*<br>▶ *At sikre, at databehandleren opbevarer fortegnelsen skriftligt, herunder elektronisk.*<br>▶ *At sikre, at databehandleren kan stille fortegnelsen til rådighed for tilsynsmyndigheden.* | | |
| **Kontrolaktivitet** | **Test udført af BDO** | **Resultat af test** |
| **Fortegnelse over kategorier af behandlingsaktiviteter**<br>▶ Bellcom har udarbejdet en fortegnelse over behandlingsaktiviteter som databehandler.<br>▶ Bellcom foretager en risikovurdering for hver behandling.<br>▶ Bellcom ajourfører fortegnelsen løbende og mindst én gang årligt. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspicereret fortegnelse og observeret, at Bellcom ajourfører behandlingsaktiviteter, herunder har risikovurderet behandlingsaktiviteterne.<br><br>Vi har inspicereret fortegnelsen, og observeret, at den er opdateret i december 2019. | Ingen afvigelser konstateret. |
| **Opbevaring af fortegnelsen**<br>▶ Bellcom opbevarer fortegnelsen elektronisk. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspicereret Bellcoms opbevaring og observeret, at fortegnelsen opbevares elektronisk. | Ingen afvigelser konstateret. |
| **Datatilsynets adgang til fortegnelsen**<br>▶ Bellcom udleverer fortegnelsen på anmodning fra en tilsynsmyndighed. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspicereret Bellcoms procedure og observeret, at databehandleren stiller alle ressourcer til rådighed for tilsynsmyndighed.<br><br>Vi har ikke kunnet efterprøve disse procedurer, da der ikke har været anmodning fra tilsynsmyndighed. | Ingen afvigelser konstateret. |

## Artikel 33, stk. 2: Underretning om brud på persondatasikkerheden

**Kontrolmål**

- *At sikre, at databehandleren uden unødig forsinkelse underretter den dataansvarlige om brud på persondatasikkerheden.*
- *At sikre, at den dataansvarlige underrettes om alle nødvendige oplysninger, så bruddet kan vurderes med henblik på anmeldelse til tilsynsmyndigheden og underretning til den registrerede.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Underretning om brud på persondatasikkerheden**<br><br>▶ Bellcom har udarbejdet og implementeret procedurer for håndtering af informationssikkerhedshændelser og brud.<br>▶ Alle informationssikkerhedshændelser og brud på persondatasikkerheden, herunder svagheder, rapporteres årligt til beredskabsledelsen.<br>▶ Medarbejdere er forpligtet til at rapportere informationssikkerhedsbrud til informationssikkerhedskoordinatoren.<br>▶ Alle medarbejdere og eksterne kontrahenter har pligt til at rapportere observerede svagheder eller sårbarheder i it-systemer og it-services til informationssikkerhedskoordinatoren. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret procedure for underretning om brud på persondatasikkerheden og observeret, at Bellcom skal underrette dataansvarlig ved brud på sikkerheden.<br><br>Vi har ved stikprøvevis interviewet udvalgt medarbejder og observeret, at medarbejder vil rapportere informationssikkerhedsbruddet til informationssikkerhedskoordinatoren.<br><br>Vi har stikprøvevis udvalgt underretning om brud på persondatasikkerheden, og observeret, at medarbejder har rapporteret informationssikkerhedsbrud. | Ingen afvigelser konstateret. |
| **Identifikation af brud på persondatasikkerheden**<br><br>▶ Dataansvarlige orienteres direkte eller via nyhedsbrev om aktivering af beredskab.<br>Informationen indeholder:<br>• En kort beskrivelse af hændelsen<br>• Sandsynlige konsekvenser af hændelsen<br>• De aktive handlinger der foretages for udbedring.<br>• Forventet udbedringstid Tidspunktet for næste<br>• orientering.<br>• Oplysninger på kontaktperson hos Bellcom, hvor yderligere oplysninger kan indhentes.<br>• De foranstaltninger der er truffet for at imødegå lignende hændelser. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret hændelser for brud på persondatasikkerheden og observeret, at Bellcom har orienteret dataansvarlig og beskrevet informationssikkerhedshændelsen. | Ingen afvigelser konstateret. |

| Artikel 33, stk. 2: Underretning om brud på persondatasikkerheden | | |
|---|---|---|
| **Kontrolmål**<br>▶ *At sikre, at databehandleren uden unødig forsinkelse underretter den dataansvarlige om brud på persondatasikkerheden.*<br>▶ *At sikre, at den dataansvarlige underrettes om alle nødvendige oplysninger, så bruddet kan vurderes med henblik på anmeldelse til tilsynsmyndigheden og underretning til den registrerede.* | | |
| **Kontrolaktivitet** | **Test udført af BDO** | **Resultat af test** |
| **Registrering af brud på persondatasikkerheden**<br><br>▶ Alle informationssikkerhedshændelser og brud på persondatasikkerheden, herunder svagheder registreres i en log. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret databrudsloggen og observeret, at informationssikkerhedshændelser og brud på persondatasikkerheden logges. | Ingen afvigelser konstateret. |

**BDO STATSAUTORISERET REVISIONSAKTIESELSKAB**

**KYSTVEJEN 29**
**8000 AARHUS C**

**CVR-NR. 20 22 26 80**