KOMBIT

Version 2.2

Instruks til systemspecifik ISAE 3000-erklæring GDPR

Indholdsfortegnelse

1. Formål

Denne instruks er udarbejdet til brug for KOMBITs kontrakter med Leverandører om levering af drift, vedligeholdelse mm. af de enkelte it-systemer (i de enkelte kontrakter benævnt "Systemet") og anvendes for at sikre, at KOMBIT på vegne af de dataansvarlige (typiske kommunerne) kan føre tilsyn med, at Leverandørerne overholder de indgåede underdatabehandleraftaler, udvalgte sikkerhedskrav i kontrakten samt princippet om privacy-by-design.

Instruksen skal følges af Leverandørerne ved levering af systemspecifikke ISAE 3000 revisionserklæringer under den enkelte kontrakt med KOMBIT.

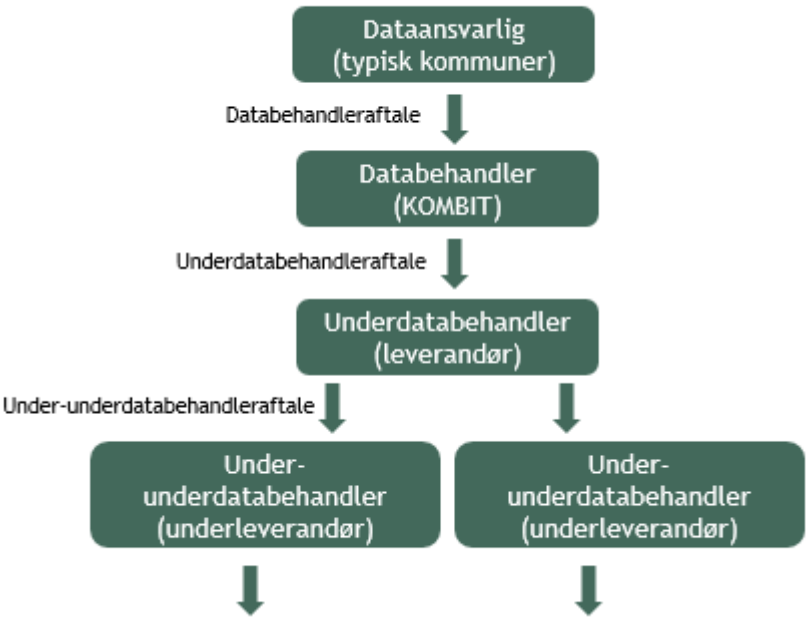
Alle revisionserklæringer skal være afgivet med en høj grad af sikkerhed. Revisionserklæringerne skal være stilet til både KOMBIT og de dataansvarlige.

2. Roller og Ansvar

Det er forudsat, at data, der behandles i Systemet, i mange tilfælde vil være personoplysninger i henhold til databeskyttelseslovgivningen.

Leverandøren og dennes Revisor skal sikre, at revisionserklæringen skal dække alle led i databehandlerkæden. Revisionserklæringen skal tydeligt dokumentere, at der er ført kontrol med alle underdatabehandlere enten via helheds- eller partielmetoden. Leverandøren skal udarbejde en retvisende oversigt over de væsentligste komplementerende kontroller. Det forventes, at afsnittet "Komplementerende kontroller" opdeles, således at det er tydeligt hvilke kontroller, der vedrører KOMBIT og hvilke kontroller, der vedrører den dataansvarlige.

Nedenstående figur illustrerer Leverandørens rolle som leverandør og underdatabehandler.



Der er indgået databehandleraftale mellem de(n) dataansvarlige og KOMBIT (som databehandler) og en underdatabehandleraftale mellem KOMBIT og Leverandøren (som underdatabehandler). Underdatabehandleraftalen mellem KOMBIT og Leverandøren afspejler de forpligtelser, der er forudsat i databehandleraftalen mellem de(n) dataansvarlige og KOMBIT.

Når en dataansvarlig overlader behandling af personoplysninger til andre, skal der føres tilsyn med, at de indgåede aftaler overholdes, og at databehandlere (og underdatabehandlere) har gennemført de aftalte tekniske og organisatoriske sikkerhedsforanstaltninger jf. underdatabehandleraftalen og kontrakten.

Til brug for KOMBITs og de(n) dataansvarliges tilsyn med Leverandøren (underdatabehandler) og dennes underleverandører (under-underdatabehandlere) skal Leverandøren afgive en **systemspecifik ISAE 3000 erklæring med høj grad af sikkerhed** fra en statsautoriseret revisor.

Erklæringen skal tage udgangspunkt i nedennævnte kontroller, som KOMBIT anser for værende fyldestgørende som dokumentation for overholdelse af databehandleraftalen mellem KOMBIT og de(n) dataansvarlige. Leverandøren og revisor skal i det omfang, det vurderes, at nedennævnte kontroller er utilstrækkelige, tilføje yderligere relevante kontroller. Kontrolmål må ikke slettes og i det omfang kontrollen anses for ikke relevant, skrives forklaring på dette.

Erklæringen skal være en systemspecifik erklæring med høj grad af sikkerhed.

I tillæg til erklæringen skal leverandøren udlevere en oversigt fra revisor over revisors findings, som ikke indgår i revisionserklæringen (prioritet 3 findings) som følge af, at disse vurderes at udgøre en mindre risiko/svaghed. Listen med revisors prioritet 3 findings skal give KOMBIT et mere komplet overblik over svagheder i Systemet.

3. Proces for udarbejdelse af erklæringen

3.1 Omfang af erklæringen

Leverandøren skal i forbindelse med udarbejdelsen af ISAE 3000-erklæringen sammen med KOMBIT og revisor på 3-partsmøder indkaldt af Leverandøren, foretage nedenstående:

- Indledningsvist gennemgå den indgåede underdatabehandleraftale mellem KOMBIT og Leverandøren med særligt fokus på de forhold, som er relevante i forbindelse med Leverandørens leverancer under kontrakten om Systemet.

- Identificere eventuelle Underleverandører hos Leverandøren (under-underdatabehandlere), som behandler personoplysninger i forbindelse med Leverandørens leverancer under kontrakten om Systemet med henblik på at sikre, at Leverandøren foretager en løbende opfølgning over for disse. De indgåede underdatabehandleraftaler skal indeholde en oversigt over godkendte under-underdatabehandlere. Under-underdatabehandlere opføres i en liste under Leverandørens beskrivelse af Systemet.

- Identificere eventuelle Underleverandører hos Leverandøren som kun anvendes som fysiske colocation providere (colocationleverandører) og (som således ikke behandler personoplysninger i forbindelse med Leverandørens leverancer under kontrakten om Systemet) med henblik på at sikre, at Leverandøren foretager en løbende opfølgning over for disse. Colocation provider opføres i en liste i Leverandørens beskrivelse af Systemet som serviceunderleverandør.

- Gennemgå Leverandørens processer og systemanvendelse med henblik på at identificere i hvilket omfang og hvordan, der behandles personoplysninger i forbindelse med Leverandørens leverancer under kontrakten om Systemet herunder beskrive Leverandørens procedure for

håndtering af informationssikkerhedshændelser, som forventes at fremgå i sektion 3 af revisionserklæringen.

- Gennemgå databeskyttelsesforordningen (GDPR) og databeskyttelsesloven med henblik på at identificere hvilke områder/kontrolmål i denne instruks, der må forventes at være relevante i erklæringen, jf. den indgåede underdatabehandleraftale. I tilknytning hertil udarbejdes en struktur for systembeskrivelsen i erklæringen. Vurderes det, at konkrete områder/kontrolmål ikke er relevante for revisionen, skal området/kontrolmålet bibeholdes i erklæringen, og det skal begrundes i erklæringen, hvorfor området/kontrolmålet ikke er relevant. Eksisterer der forhold, som efter revisors vurdering er væsentlige, og som ikke er indeholdt i områderne/kontrolmålene i denne instruks, skal disse medtages i den afgivne erklæring.

- Gennemgå Leverandørens kontroller inden for de identificerede områder/kontrolmål, som ISAE 3000-erklæringen skal omfatte, herunder den dokumentation som skal foreligge i forbindelse med revision heraf.

- Eventuelle afvigelser fra instruksen skal begrundes i revisionserklæringen, for at skabe transparens.

- Indarbejde KOMBITs skriftlige ønsker til specifikke emner, kontroller og områder, som skal med i revisionserklæringen.

- Tilrettelægge en proces, som sikrer involvering af KOMBIT inden underskrift af revisionserklæring, med henblik på at afklare eventuelle anmærkninger fra revisor i form af et udkast.

3.2 Anvendt metode for udarbejdelse af erklæringen

Det skal af hver erklæring detaljeret fremgå, hvilke revisionshandlinger der er udført for at nå til erklæringens konklusioner. Er der afdækket risici og/eller svagheder hos Leverandøren, herunder i relation til overholdelse af persondatalovgivningen, driftsmiljøet og/eller sikkerhedsprocedurer, skal disse detaljeret fremgå af erklæringen.

I det omfang, der anvendes under-underdatabehandlere, kan Leverandøren vælge enten direkte at inkludere under-underdatabehandlerne i revisionserklæringen (helhedsmetoden) eller udelade disse fra erklæringen (partielmetoden).

Hvis partielmetoden vælges, skal revisionserklæringen som minimum indeholde kontrolmål og kontroller til monitorering af, om under-underdatabehandlerne opfylder deres forpligtelser overfor KOMBIT og de dataansvarlige. Denne monitorering af under-underdatabehandlere skal omfatte indhentelse og gennemgang af revisorerklæringer med tilsvarende indhold og detaljeringsgrad som i en ISAE 3000 revisionserklæring. Erklæringerne fra under-underdatabehandlerne skal enten omfatte samme periode eller en periode, der slutter højst 3 måneder tidligere end Leverandørens egen ISAE 3000 revisionserklæring.

Revisionserklæringen skal endvidere som minimum indeholde kontrolmål og kontroller til monitorering af, om fysiske colocation providere opfylder deres forpligtelser overfor KOMBIT og de dataansvarlige. Denne monitorering af serviceunderleverandører skal omfatte indhentelse og gennemgang af revisorerklæringer med tilsvarende indhold og detaljeringsgrad som i en ISAE 3000 revisionserklæring. Erklæringerne fra serviceunderleverandør skal enten omfatte samme periode eller en periode, der slutter højst 3 måneder tidligere end Leverandørens egen ISAE 3000 revisionserklæring.

3.3 Handlingsplan ved bemærkninger i erklæringen

Hvis revisionsionserklæringen indeholder bemærkninger, kommentering mv., skal Leverandøren samtidig med fremsendelsen af revisionserklæringen fremsende en fyldestgørende handlingsplan, som beskriver, hvordan og hvornår de omhandlede forhold, herunder forhold identificeret i forbindelse med revision af under-underdatabehandlere, bringes i orden. Handlingsplanen skal følge KOMBITs skabelon og opdateres løbende, så den afspejler den til enhver tid aktuelle status på udbedring af anmærkninger i revisionserklæringen. Når forholdet er bragt i orden, skal revisor supplere sin erklæring hermed.

De dataansvarlige har en forpligtigelse til at føre tilsyn og har derfor ret til at få Leverandørens ISAE 3000-erklæring og erklæringer fra under-underdatabehandlere udleveret.

4. Kontrolmål og aftalte kontroller

Følgende kontroller, som tager udgangspunkt i ISAE 3000 FSR standarden, anser KOMBIT for værende fyldestgørende dokumentation i forhold til overholdelse af databehandleraftalen mellem KOMBIT og Kommunerne. Hvis Leverandøren og/eller revisor vurderer yderligere kontroller, vil være nødvendige, tilføjes disse efter aftale med KOMBIT.

Kontrolmål A **Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående underdatabehandleraftale.**		
Nr.	*Underdatabehandlers kontrolaktivitet*	*Revisors udførte test*
A1	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 instruks eller ændringer i databehandlingen. Inspiceret, at procedurer er opdateret.

A2	Underdatabehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra databehandleren KOMBIT.	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 instruks eller ændringer i databehandlingen. Inspiceret, at procedurer er opdateret.
A3	Underdatabehandleren underretter omgående databehandleren KOMBIT, hvis en instruks efter underdatabehandlerens 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 databehandleren KOMBIT i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Inspiceret, at databehandleren KOMBIT er underrettet i tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.

A4	Underdatabehandler opdaterer løbende fortegnelse over behandling af personoplysninger.	Inspiceret, at der foreligger formaliserede procedurer for løbende opdatering af fortegnelsen over behandling af personoplysninger. Inspiceret, at fortegnelse over behandling af personoplysninger er ajour

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at underdatabehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**		
Nr.	*Underdatabehandlers kontrolaktivitet*	*Revisors udførte test*
B1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med underdatabehandleraftalen. 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 underdatabehandleraftalen med KOMBIT, at der er etableret de aftalte sikringsforanstaltninger.

B2	Underdatabehandleren 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 databehandler (KOMBIT) aftalte sikringsforanstaltninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at underdatabehandler 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 underdatabehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Inspiceret, at underdatabehandler har implementeret de sikringsforanstaltninger, der er aftalt med KOMBIT.
B3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antimalware, herunder antivirus, som løbende opdateres.	Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antimalware, herunder antivirus. Inspiceret, at antimalware, herunder antivirus er opdateret.

B4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall, herunder anvendelsen af antimalware inklusiv antivirus. Underdatabehandler anvender DDoS mitigering.	Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall, der anvender antimalware inklusiv antivirus. Inspiceret, at firewall er konfigureret i henhold til intern politik. Inspiceret at DDoS mitigering er konfigureret i henhold til intern politik.
B5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Alle netværkskomponenter er redundante f.eks. i kraft af to eller flere datacentre.	Inspiceret, at 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. Inspiceret dokumentation for teknisk infrastruktur. Inspiceret procedure for netværksstyring.

B6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor. Der anvendes detaljeret brugerstyring i systemet så der sikres least-privilege adgang. Der må ikke anvendes fællesbrugerkonto på systemet. Der sikres funktionsadskillelse i systemet.	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 ved stikprøve, at leverandøren har foretaget en løbende gennemgang af hvorvidt brugere med adgang til systemet har et arbejdsbetinget behov samt opfølgning på denne gennemgang. Inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger. Inspiceret ved en stikprøve på brugeres adgange til systemer og databaser, at de er begrænset til medarbejdernes arbejdsbetingede behov. Inspiceret udtræk og løbende gennemgang af brugere som har adgang til systemet og infrastrukturen. Inspiceret procedure for adgangsstyring, herunder anvendelsen af personlige brugere og sikring af least-privilege adgange. Inspiceret procedure for sikring af funktionsadskillelse.

		Inspiceret ved stikprøve at funktionsadskillelse er effektiv.
B7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter eksempelvis: • DDoS • Anti virus og malware • Jumpservere • IP spoofing	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 alarmer er sket opfølgning, samt at forholdet er meddelt til databehandleren (KOMBIT) i overensstemmelse med kontrakten.

B8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail. Politikker for håndtering og kopiering af forretningsdata; Som udgangspunkt holdes al forretningsdata udelukkende i systemet og kopieres ikke. Hvis kopiering er nødvendig, definerer underdatabehandlerens sikkerhedshåndbog politikker for kopiering – herunder korttidsopbevaring og kryptering jf. underdatabehandleraftalen.	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 databehandleren KOMBIT er orienteret herom i overensstemmelse med kontrakten. Inspiceret overholdelse af politikker for håndtering og kopiering af forretningsdata.

B9	Der er etableret logning i systemer, databaser og netværk af følgende 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 o 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 der foretages logning af brugeraktiviteter, således det kan dokumenteres, hvem som har set hvilke data og hvornår. 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 et relevant antal dages logning, at 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 et relevant antal dages logning, at der er dokumentation for den foretagne opfølgning på aktiviteter udført af systemadministratorer og andre med særlige rettigheder.

B10	Personoplysninger, der anvendes til udvikling, test, supportsager eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage dens dataansvarliges 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 udviklings- og testdatabaser, at personoplysninger heri er pseudonymiseret eller anonymiseret. Inspiceret ved en stikprøve på udviklings- og testdatabaser, hvor personoplysninger ikke er pseudonymiseret eller anonymiseret, at dette er sket efter aftale med databehandleren KOMBITog på dennes vegne. Inspiceret procedure og dokumentation for håndtering af supportsager.
B11	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 KOMBIT i overensstemmelse med kontrakten.

B12	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.
B13	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, regelmæssig revurdering og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Inspiceret ved en stikprøve på medarbejderes adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov. Inspiceret ved en stikprøve på fratrådte 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.

B14	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 højrisiko for de registrerede, alene kan ske ved anvendelse af to-faktor autentifikation.
B15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Det/de anvendte datacentre er beskyttet mod relevante trusler som f.eks. brand, overophedning, vandskade, magnetisme, forsyningssvigt, tyveri eller hærværk, svarende til leverandørens trusselsvurdering.	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. Inspiceret at det/de anvendte datacentre er beskyttet mod relevante trusler som f.eks. brand, overophedning, vandskade, magnetisme, forsyningssvigt, tyveri eller hærværk.

B16	Der foretages løbende backup eller sikring vha. redundans eller lignende af de vigtigste og mest essentielle data i systemet, så der altid er mindst 2 kopier af alle data. Kontrol af at backuppen er læsbar, skrivebeskyttet, har det rette omfang og kan reetableres	Inspiceret konfiguration af backup i henhold til politik. Inspiceret skriftlige procedurer for backup. Inspiceret ved stikprøve, at der foretages backup i overensstemmelse med kontrakten. Inspiceret skriftlige procedurer for kontrol af, at backuppen er læsbar, skrivebeskyttet, har det rette omfang og kan reetableres. Inspiceret ved stikprøve, at der løbende foretages kontrol af, at backuppen er læsbar, skrivebeskyttet, har det rette omfang og kan reetableres.
B17	Al data opbevares georedundant i flere datacentre.	Inspiceret dokumentation for teknisk infrastruktur i forhold til georedundant opbevaring.
B18	Underdatabehandler skal på alle relevante områder have dokumenteret tekniske sikkerhedsforanstaltninger jf. ISO 27002.	Inspiceret dokumentation for, at underdatabehandler har foretaget mapning eller anden vurdering af relevante områder i ISO 27002.

B19	Der skal være opdaterede og effektive beredskabsplaner og -procedurer, der sikrer genetablering af personoplysninger og adgange, inden for de i kontrakten fastsatte tidsfrister i tilfælde af driftsafbrydelser/forstyrrelser. Effektiviteten af beredskabsplaner og procedurer for genetablering af personoplysninger og adgang skal regelmæssigt afprøves og evalueres.	Inspiceret dokumentation for opdaterede og effektive beredskabsplaner og -procedurer. Inspiceret procedurer for regelmæssig afprøvning og evaluering af beredskabsplaner og procedurer for genetablering. Inspiceret ved stikprøve at beredskabsplaner og procedurer for genetablering løbende afprøves og evalueres.

Kontrolmål C **Der efterleves procedurer og kontroller, som sikrer, at underdatabehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**		
Nr.	*Underdatabehandlers kontrolaktivitet*	*Revisors udførte test*
C1	Underdatabehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder underdatabehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst én gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Inspiceret, at der foreligger en opdateret informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder underdatabehandlerens medarbejdere.
C2	Underdatabehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med den indgåede underdatabehandleraftale.	Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i den indgåede underdatabehandleraftale. Inspiceret ved en stikprøve på underdatabehandleraftalen, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.

C3	Der udføres en efterprøvning af underdatabehandlerens medarbejdere i forbindelse med ansættelse i form af baggrundstjek. Efterprøvningen er beskrevet i relevant omfang kan inkludere indhentning af: • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbeviser	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af underdatabehandlerens medarbejdere i forbindelse med ansættelse. Inspiceret ved en stikprøve, at proceduren for efterprøvning af medarbejdere i relevant omfang er efterlevet. Inspiceret ved en stikprøve på nyansatte medarbejdere i erklæringsperioden, at der er dokumentation for, at efterprøvningen i relevant omfang har evt. omfattet: • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbeviser
C4	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 nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere har underskrevet en fortrolighedsaftale. Inspiceret ved en stikprøve på nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere er blevet introduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling, samt anden relevant information.

C5	Ved fratrædelse er der hos underdatabehandleren 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 fratrådte medarbejdere i erklæringsperioden, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.
C6	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, underdatabehandleren 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 fratrådte medarbejdere i erklæringsperioden, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt ved medarbejderens ansættelsesophør.
C7	Der gennemføres løbende awareness træning af underdatabehandlerens medarbejdere i relation til it-sikkerhed generelt, samt behandlingssikkerhed i relation til personoplysninger.	Inspiceret, at underdatabehandleren 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.

C8	Underdatabehandler skal på alle relevante områder have dokumenteret organisatoriske sikkerhedsforanstaltninger jf. ISO 27002.	Inspiceret dokumentation for at underdatabehandler har foretaget mapning eller anden vurdering af relevante områder i ISO 27002.

Kontrolmål D **Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med databehandleren KOMBIT.**		
Nr.	*Underdatabehandlers kontrolaktivitet*	*Revisors udførte test*
D1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med underdatabehandleraftalen. 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 underdatabehandleraftalen. Inspiceret, at procedurerne er opdateret.

D2	Der er aftalt specifikke krav til underdatabehandlerens opbevaringsperioder og sletteregler, jf. kontrakten med bilag mellem KOMBIT og leverandøren.	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til underdatabehandlerens opbevaringsperioder og sletteregler. Inspiceret ved en stikprøve på databehandlinger fra underdatabehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder. Inspiceret ved en stikprøve på databehandlinger fra underdatabehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger er slettet i overensstemmelse med de aftalte sletteregler.
D3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til underdatabehandleraftalen: • 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. Inspiceret ved en stikprøve på ophørte databehandlinger i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.

Kontrolmål E **Der efterleves procedurer og kontroller, som sikrer, at underdatabehandleren alene opbevarer personoplysninger i overensstemmelse med underdatabehandleraftalen.**		
Nr.	*Underdatabehandlers kontrolaktivitet*	*Revisors udførte test*
E1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med underdatabehandleraftalen. 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 underdatabehandleraftalen. Inspiceret, at procedurerne er opdateret. Inspiceret ved en stikprøve på databehandlinger fra underdatabehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til underdatabehandleraftalen.
E2	Underdatabehandlerens databehandling inklusive opbevaring må kun finde sted på de godkendte lokaliteter, lande eller landområder, jf. underdatabehandleraftalen.	Inspiceret, at underdatabehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Inspiceret ved en stikprøve på databehandlinger fra underdatabehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af underdatabehandleraftalen – eller i øvrigt er godkendt af databehandleren KOMBIT.

Kontrolmål F **Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte under-underdatabehandlere, samt at underdatabehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.**		
Nr.	*Underdatabehandlers kontrolaktivitet*	*Revisors udførte test*
F1	Der foreligger skriftlige procedurer, som indeholder krav til underdatabehandleren ved anvendelse af under-underdatabehandlere, herunder krav om under-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 under-underdatabehandlere, herunder krav om under-underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.
F2	Underdatabehandleren anvender alene under-underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af databehandleren KOMBIT, jf. underdatabehandleraftalen.	Inspiceret, at underdatabehandleren har en samlet og opdateret oversigt over anvendte under-underdatabehandlere. Inspiceret ved en stikprøve på under-underdatabehandlere fra underdatabehandlerens oversigt over under-underdatabehandlere, at der er dokumentation for, at under-underdatabehandlerens databehandling fremgår af underdatabehandleraftalen – eller i øvrigt er godkendt af databehandleren KOMBIT.

F3	Ved ændringer i anvendelsen af generelt godkendte under-underdatabehandlere, underrettes databehandleren KOMBIT rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra underdatabehandleren. Ved ændringer i anvendelse af specifikt godkendte under-underdatabehandlere, er dette godkendt af databehandleren KOMBIT.	Inspiceret, at der foreligger formaliserede procedurer for underretning til databehandleren KOMBIT ved ændringer i anvendelse af under-underdatabehandlere. Inspiceret dokumentation for, at databehandleren KOMBIT er underrettet ved ændring i anvendelse af under-underdatabehandlerne i erklæringsperioden.
F4	Underdatabehandleren har pålagt under-underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i underdatabehandleraftalen.	Inspiceret, at der foreligger underskrevne under-underdatabehandleraftaler med anvendte under-underdatabehandlere, som fremgår af underdatabehandlerens oversigt. Inspiceret ved en stikprøve på under-underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i underdatabehandleraftalen.
F5	Underdatabehandleren har en oversigt over godkendte under-underdatabehandlere med angivelse af: • Navn • CVR nr. • Adresse • Beskrivelse af behandlingen	Inspiceret, at underdatabehandleren har en samlet og opdateret oversigt over anvendte og godkendte under-underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte under-underdatabehandlere.

F6	Underdatabehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte under-underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Databehandleren KOMBIT orienteres løbende om den opfølgning, der er foretaget hos under-underdatabehandleren. Underdatabehandleren foretager gennemgang af og opfølgning på de dækkende revisionserklæringer/rapporter i erklæringsperioden fra de enkelte under-underdatabehandlere og colocationleverandører med henblik på at vurdere, om erklæringerne dokumenterer efterlevelse af de i underdatabehandleraftalerne anførte krav.	Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos under-underdatabehandlerne jf. oversigten over under-underdatabehandlere i Leverandørens beskrivelse af Systemet og overholdelse af under-underdatabehandleraftalerne. Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte under-underdatabehandler jf. oversigten over under-underdatabehandlere i Leverandørens beskrivelse af Systemet og den aktuelle behandlingsaktivitet hos denne. Inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte under- og colocationleverandører jf. oversigterne over under-underdatabehandlere og colocationleverandører i Leverandørens beskrivelse af Systemet, tredjelands overførselsgrundlag og lignende. Inspiceret dokumentation for, at information om opfølgning hos under-underdatabehandlere og colocationleverandører jf. oversigterne over under-underdatabehandlere og colocationleverandører i Leverandørens beskrivelse af Systemet meddeles databehandleren KOMBIT, således denne kan tilrettelægge eventuelt tilsyn.

		Inspiceret procedure og dokumentation for gennemgang af revisionserklæringer/SOC 2 rapporter for under-underdatabehandlere og colocationleverandører jf. oversigterne over under-underdatabehandlere og colocationleverandører i Leverandørens beskrivelse af Systemet.

Kontrolmål G **Der efterleves procedurer og kontroller, som sikrer, at underdatabehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med underdatabehandleraftalen på baggrund af et gyldigt overførselsgrundlag.**		
Nr.	*Underdatabehandlers kontrolaktivitet*	*Revisors udførte test*
G1	Der foreligger skriftlige procedurer, som indeholder krav om, at underdatabehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med underdatahandleraftalen 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 databehandleren KOMBIT, på baggrund af et gyldigt overførselsgrundlag. Inspiceret, at procedurerne er opdateret.
G2	Underdatabehandler må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra KOMBIT i rollen som databehandler.	Inspiceret, at underdatabehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer. Inspiceret ved en stikprøve på dataoverførsler fra underdatabehandlerens oversigt over overførsler, at der er dokumentation for, at overførslen er aftalt med databehandleren KOMBIT i underdatabehandleraftalen eller senere godkendt.

G3	Underdatabehandleren 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 dataoverførsler fra underdatabehandlerens oversigt over overførsler, at der er dokumentation for et gyldigt overførselsgrundlag i underdatabehandleraftalen, samt at der kun er sket overførsler, i det omfang dette er aftalt med databehandleren KOMBIT.

Kontrolmål H **Der efterleves procedurer og kontroller, som sikrer, at underdatabehandleren kan bistå KOMBIT i rollen som databehandler med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.**		
Nr.	*Underdatabehandlers kontrolaktivitet*	*Revisors udførte test*
H1	Der foreligger skriftlige procedurer, som indeholder krav om, at underdatabehandleren 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 underdatabehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.
H2	Underdatabehandleren 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. ELLER HVIS BISTAND I PERIODEN: Inspiceret, at dokumentation for anmodninger om bistand fra den dataansvarlige i relation til

		udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede er korrekt og rettidigt gennemført.

Kontrolmål I **Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale med KOMBIT.**		
Nr.	*Underdatabehandlers kontrolaktivitet*	*Revisors udførte test*
I1	Der foreligger skriftlige procedurer, som indeholder krav om, at underdatabehandleren skal underrette databehandleren KOMBIT 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 databehandleren KOMBIT ved brud på persondatasikkerheden. Inspiceret, at proceduren er opdateret.
I2	Underdatabehandleren 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 underdatabehandler 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.

I3	Underdatabehandleren har ved eventuelle brud på persondatasikkerheden underrettet databehandleren KOMBIT uden unødig forsinkelse og senest 1 time efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos underdatabehandleren eller en under-underdatabehandler.	Inspiceret, at underdatabehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Forespurgt under-underdatabehandlerne, om de har konstateret nogen brud på persondatasikkerheden i erklæringsperioden Inspiceret, at underdatabehandleren har medtaget eventuelle brud på persondatasikkerheden hos under-underdatabehandlere i underdatabehandlerens oversigt over sikkerhedshændelser. Inspiceret, at samtlige registrerede brud på persondatasikkerheden hos underdatabehandleren eller under-underdatabehandlerne er meddelt databehandleren KOMBIT uden unødig forsinkelse og senest 1 time efter, at underdatabehandleren er blevet opmærksom på brud på persondatasikkerheden.

I4	Underdatabehandleren har etableret procedurer for bistand til databehandleren KOMBIT samt 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 databehandleren KOMBIT 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

5. Versionshistorik

Dato for revidering:	Revideret af:	Rettelse:
16/08/2023	Service Management	
22/09/2023	Service Management	Opdatering af B18
27/06/2025	Service Management	Opdatering afsnittene om 'Roller og ansvar' samt 'Proces for udarbejdelse af erklæringen'. Tilføjet kontrol B19 (beredskabsplan) og C8 (organisatoriske sikkerhedsforanstaltninger jf. ISO27002) Opdatering B5, B15, B16 og C3. Opdatering testbeskrivelser for kontrol A4, B5, B6, B13, B15, B16 og C3. Korrektur og præciseringer