DATATILSYNET

Bilag 2: Spørgsmål med hjælpetekster

6. juli 2021

J.nr. 2021-429-0001
Dok.nr. 369005
JIS

Spm. ID	Spørgsmål	Hjælpetekster og henvisninger
1.	**Organisationsprofil**	
1.1	Er organisationen etableret i lande uden for Danmark, men inden for EU?	**Hjælpetekst** Her tænkes særligt på afdelinger, butikker, lokaler eller lignende, hvorfra der drives virksomhedsaktiviteter.
1.2	Er organisationen etableret i lande uden for EU?	**Hjælpetekst** Her tænkes særligt på afdelinger, butikker, lokaler eller lignende, hvorfra der drives virksomhedsaktiviteter.
2.	**Aktiviteter**	
2.1	Hvor mange it-systemer (informationssystemer) anvender organisationen?	**Hjælpetekst** Det kan i praksis være vanskeligt at afgøre, hvad der er et selvstændigt 'it-system', herunder hvor grænserne går mellem flere sammenhængende netværk, systemer og databaser. Et it-system anvendes typisk til indsamling, systematisering, opbevaring, ændring, søgning, brug, videregivelse, overladelse, sammenstilling, samkøring, distribution og sletning af personoplysninger. Det kan bl.a. være tale om sagsbehandlingssystemer, kunde- og leverandørsystemer, økonomi- og betalingssystemer, leverance- og produktionssystemer, webløsninger mv. Det er ikke afgørende, om systemet drives af organisation selv, eller om der anvendes underleverandører, herunder cloud-leverandører. Der efterspørges her et omtrentligt (cirka) bud på, hvor mange systemer – der ud fra organisationens egen forståelse – kan karakteriseres som 'it-systemer'. Svaret skal angives inden for de mulige intervaller.
2.2	Har organisationen etableret et eller flere serverrum?	**Hjælpetekst** Med 'serverrum' menes lokaler, som er særligt indrettet til opstilling og drift af servere – typisk med faciliteter som f.eks. kølings- og ventilationsanlæg, sikring mod brand og oversvømmelser, nødstrømsanlæg og med særlig adgangskontrol således, at kun få udvalgte medarbejdere har adgang til rummet.

2.3	Hvor mange registrerede behandler organisationen oplysninger om?	**Hjælpetekst** Den registrerede er en enhver identificeret eller identificerbar fysisk person, om hvem der behandles personoplysninger. Det kan f.eks. være ansatte, samarbejdspartnere, kunder, borgere og studerende/elever. Der efterspørges her et omtrentligt (cirka) bud på, hvor mange registrerede personer – der ud fra organisationens egen forståelse – behandlers oplysninger om. Svaret skal angives inden for de mulige intervaller. **Henvisninger** Databeskyttelsesforordningens artikel 4, nr. 1
2.4	Behandler organisationen følsomme personoplysninger om kunder/borgere (særlige kategorier af personoplysninger)?	**Hjælpetekst** Følsomme personoplysninger er udtrykkeligt afgrænset i databeskyttelsesforordningen, og adgangen til at behandle sådanne oplysninger er snævrere end ved almindelige personoplysninger. Følsomme oplysninger er oplysninger om: • Race og etnisk oprindelse • Politisk overbevisning • Religiøs eller filosofisk overbevisning • Fagforeningsmæssige tilhørsforhold • Genetiske data • Biometriske data med henblik på entydig identifikation • Helbredsoplysninger • Seksuelle forhold eller seksuel orientering. Læs mere om de forskellige kategorier af personoplysninger her: https://www.datatilsynet.dk/hvad-siger-reglerne/grundlaeggende-begreber-/hvad-er-personoplysninger **Henvisninger** Databeskyttelsesforordningens artikel 9, stk. 1.
2.5	Stiller organisationen it-systemer til rådighed for andre virksomheders/myndigheders behandling af personoplysninger?	**Hjælpetekst** Der tænkes særligt på organisationer, som stiller it-systemer (it-løsninger) til rådighed for virksomheder/myndigheder med henblik på, at disse virksomheder/myndigheder kan opbevare og behandle personoplysninger i de pågældende systemer. Det vil typisk være tilfældet i situationer, hvor organisationen (eller en evt. underleverandør) drifter og hoster selve it-systemet, og hvor virksomhederne/myndighederne typisk via en fjernadgang anvender systemet til behandling af egne personoplysninger. Organisationen "ejer" således ikke selv de pågældende personoplysninger og kan alene behandle oplysningerne efter instruks fra den relevante virksomhed/myndighed. Organisationen kan i sådanne situationer karakteriseres som en såkaldt databehandler. **Henvisninger** Databeskyttelsesforordningens artikel 4. nr. 8

3.	Organisering og informationssikkerhed	
3.1	Har organisationen udpeget en person, som er ansvarlig for informationssikkerhed?	**Hjælpetekst** Som 'ansvarlig for informationssikkerhed' vil en organisation typisk have udpeget en it-chef, digitaliseringschef, CISO eller CTO, men det udelukker ikke, at ansvaret kan være placeret hos andre medarbejdere. Alt efter organisationens størrelse og kompleksitet vil det styrke arbejdet med informationssikkerheden, hvis der er en klar ansvarsfordeling i forhold til, hvem der skal varetage de enkelte sikkerhedsopgaver. **Henvisninger** ISO 27001 - A.6.1.1 ISO 27002 - 6.1.1
3.2	Følger organisationen én eller flere ledelsesstandarder (f.eks. ISO, ISAE, NIST) for informationssikkerhed?	**Hjælpetekst** En standard for informationssikkerhed er normalt et rammeværktøj, som organisationer kan anvende med henblik på, at arbejdet med informationssikkerhed er dækkende. Typisk anvendte informationssikkerhedsstandarder er ISO 2700x, ISAE, COBIT og NIST. Det bemærkes, at adgangen til at se og anvende sådanne standarder typisk vil være forbundet licens- eller abonnentsomkostninger. Eksempler på standarder kan findes her: https://www.iso.org/isoiec-27001-information-security.html https://www.isaca.org/resources/cobit https://www.nist.gov/cyberframework **Henvisninger** ISO 27002 - 18.2.2
3.3	Har organisationen udarbejdet en fortegnelse (oversigt) over alle behandlingsaktiviteter?	**Hjælpetekst** En fortegnelse over behandlingsaktiviteter er en skriftlig og elektronisk oversigt, som giver organisationen et overblik over de personoplysninger, som organisationen behandler. Yderligere information om krav til fortegnelse kan findes i Datatilsynets vejledning her: https://www.datatilsynet.dk/media/6567/fortegnelse.pdf **Henvisninger**

		Databeskyttelsesforordningens artikel 30.
3.4	Har organisationen udarbejdet en politik for informationssikkerheden ved behandling af personoplysninger?	**Hjælpetekst** En informationssikkerhedspolitik fastsætter på et overordnet niveau principper for, hvad organisationen, herunder medarbejderne, skal gøre i forhold til beskyttelsen af bl.a. it-systemer, computere, mobile enheder og informationer, herunder personoplysninger. En skabelon og vejledning til informationssikkerhedspolitik kan findes her: https://sikkerdigital.dk/media/6678/it-sikkerhedspolitik.zip Mere information og anbefalinger til passende sikkerhed kan findes her: https://startvaekst.virk.dk/node/1884/security-report/recommendations/pdf **Henvisninger** ISO 27001 - A.5.1.1 ISO 27002 - 5.1.1
3.5	Følger organisationen et årshjul, som sikrer, at alle væsentlige politikker, retningslinjer mv. bliver opdateret regelmæssigt?	**Hjælpetekst** Alt efter organisationens størrelse og kompleksitet kan det være nødvendigt systematisk at kontrollere, at væsentlige politikker og retningslinjer er ajourførte og opdaterede med de faste intervaller. I et årshjul kan organisationen på overskuelig vis samle information om de aktiviteter, der skal gennemføres og fastlægge datoer og ansvar for, at aktiviteterne bliver gennemført. Med 'væsentlige politikker og retningslinjer mv.' menes dokumenter, som - efter organisationens egen opfattelse - er centrale i forhold til sikringen af informationssikkerheden og databeskyttelsen i organisationen. En 'opdatering' indebærer især, at der er taget stilling til eventuelle ændringer i organisationens aktiviteter og struktur, herunder behandlingsaktiviteter og organisationsændringer., Herudover er politikker og retningslinjer tilpasset i overensstemmelse med den gældende lovgivning, kontraktkrav og risikobillede. Med 'regelmæssigt' menes intervaller, der er passende for organisationen – typisk hvert eller hvert andet år. Intervallet kan dog være afhængigt af f.eks. kompleksiteten af organisationen og behandlingsaktiviteterne eller større organisatoriske, fysiske og it-mæssige ændringer. **Henvisninger** ISO 27001 - A.5.1.2 ISO 27002 - 5.1.2 ISO 27001 - A.18.2 ISO 27001 - 6.1 ISO 27005 ISO 31000

3.6	Bliver dokumenter omfattet af et eventuelt århus-hjul - jf. spørgsmål 3.5. - godkendt på ledelsesniveau?	**Hjælpetekst** Alt efter karakteren af en organisation og de aktiviteter en organisation udfører, vil det oftest være hensigtsmæssigt, at organisationens ledelse involverer sig i arbejdet med informationssikkerhed og databeskyttelse. Dette vil f.eks. kunne komme til udtryk ved, at ledelsen godkender væsentlige politikker, vejledninger, instrukser mv. på informationssikkerheds- og databeskyttelsesområdet. Med 'ledelsesniveau' menes den eller de personer, som har et mere overordnet ansvar for den daglige ledelse af organisationen – f.eks. en direktør eller en underdirektør. I denne sammenhæng spørges der ikke til bestyrelser eller koncernforbundne selskaber – f.eks. et moderselskab. **Henvisninger** ISO 27001 - A.5.1.2 ISO 27001 - A.18.2.2 ISO 27002 - 5.1.2 ISO 27002 - 18.2.2
4.	**Risikovurderinger**	
4.1	Har organisationen taget udtrykkeligt stilling til, hvordan relevante trusler mod informationssikkerheden vil kunne påvirke organisationen forretningsaktiviteter negativt (en forretningsmæssig risikovurdering)?	**Hjælpetekst** En 'forretningsmæssig risikovurdering' indebærer, at organisationen tager stilling til de risici, der er kritiske for virksomhedens forretningsmæssige aktiviteter (eller for myndighedernes vedkommende; for udøvelsen af myndighedsopgaver). En sådan risikovurdering indebærer også en vurdering af, hvilket sikkerhedsniveau der vil være passende (accepteret) for organisationen. En skabelon til brug for risikovurderinger og vejledning kan findes her: https://sikkerdigital.dk/media/6677/risikovurdering.zip En risikovurderingsværktøj kan findes her: https://virksomhedsguiden.dk/content/ydelser/it-risikovurderingsvaerktoej/fce38da7-025d-4326-98fe-c198f3ad8316/ **Henvisninger** ISO 27001 – 6.1 ISO 27005 ISO 31000
4.2	Har organisationen taget udtrykkeligt stilling til, hvordan relevante trusler mod informationssikkerheden vil kunne påvirke de registreredes rettigheder negativt (en databeskyttelsesretlig risikovurdering)?	**Hjælpetekst** En 'databeskyttelsesretlig risikovurdering' indebærer, at organisationen tager stilling til de risici, der er forbundet med behandlingen af personoplysninger, herunder risikoen for de registrerede. En sådan risikovurdering tager således ikke udgangspunkt i de "problemer", der kan opstå for organisationen selv, men i stedet for de "problemer", som kan opstå for de

		kunder, borgere, ansatte mv., organisationen behandler oplysninger om. Dette kan f.eks. være ringeagt og mistillid, økonomisk tab eller tab af rettigheder og muligheder. En databeskyttelsesretlig risikovurdering indebærer også en vurdering af, hvilket sikkerhedsniveau der vil være passende for beskyttelsen af de registrerede. Yderligere information om risikovurderinger kan findes her: https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed-/risikovurdering https://www.datatilsynet.dk/Media/4/8/Risikovurdering.pdf
4.3	Opdateres eventuelle skriftlige risikovurderinger regelmæssigt?	**Hjælpetekst** De interne forhold i organisationen og de eksterne forhold i omverdenen vil ændre sig med tiden, og dermed vil de fleste organisationer opleve et skiftende risikobillede – dvs. at nogle trusler vil blive mindre, mens andre vil blive større. Det er vigtigt, at risikovurderingerne afspejler dette skiftende risikobillede ved hele tiden at være retvisende. Derfor skal risikovurderinger opdateres regelmæssigt i særdeleshed ved større organisatoriske ændringer og/eller ændringer i behandlingsaktiviteter. En opdatering indebærer især, at der er taget stilling til eventuelle ændringer i trusler og risici (sandsynlighed og konsekvens), og at risikovurderingen er tilpasset i overensstemmelse med det nye trussels- og risikobillede. Med 'regelmæssigt' menes periodiske intervaller, som er passende for organisationen – typisk hvert eller hvert andet år. Intervallet kan dog være afhængigt af f.eks. kompleksiteten af organisationen og behandlingsaktiviteterne eller større organisatoriske, fysiske og it-mæssige ændringer. Yderligere information om risikovurderinger kan findes på Datatilsynets hjemmeside her: https://www.datatilsynet.dk/emner/persondatasikkerhed/risikovurdering/ https://www.datatilsynet.dk/media/7900/vejledende-tekst-om-risikovurdering.pdf **Henvisninger** ISO 27001 - 6.1 ISO 27005 ISO 31000
4.4	Bliver risikovurderinger godkendt på ledelsesniveau?	**Hjælpetekst** Med 'ledelsesniveau' menes den eller de personer, som har et mere overordnet ansvar for den daglige ledelse af (dele af) organisationen – f.eks. en direktør eller en underdirektør. I denne sammenhæng spørges der ikke til bestyrelser eller koncernforbundne selskaber – f.eks. et moderselskab. En godkendelse på ledelsesniveau kan eksempelvis komme til udtryk ved et godkendt risikovurderingsdokument, en e-mail, et mødereferat eller i en anden skriftlig og dateret form, hvor det tydeligt fremgår, at ledelse har forholdt sig til risici

		og har påtaget sig ansvaret for, at organisationen handler i overensstemmelse med de overvejelser, som fremgår af risikovurderingen. **Henvisninger** ISO 27001 - A.5.1.2 ISO 27002 - 5.1.2
5.	**Adgang til og brug af oplysninger**	
5.1	Har organisationen udarbejdet en skriftlig procedure for at tildele og nedlægge brugeradgange og -rettigheder til it-systemer, når medarbejdere ansættes eller fratræder?	**Hjælpetekst** Alt efter organisationens størrelse og kompleksitet kan det være nødvendigt at udarbejde en procedure for at administrere brugeres (f.eks. ansattes) systemadgange – f.eks. deres adgang til personoplysninger. En sådan administration af brugeradgange til personoplysninger skal være begrundet i brugernes arbejdsbetingede behov og skal forebygge, at brugerne ikke kan tilgå oplysninger, som de ikke har behov for at anvende. Med 'brugeradgange og -rettigheder' menes den opsætning af adgange til systemer og it-tjenester, der tildeles brugere, så de kan anvende systemet – ofte efter indtastning af brugernavn og kode. **Henvisninger** ISO 27001 – A.9.2 ISO 27002 – 9.2
5.2	Har organisationen en skriftlig politik for valg af adgangskoder?	**Hjælpetekst** Med 'politik' menes et dokument, som udtrykkeligt stiller krav til brugernes valg af adgangskoder. En politik bør normalt fastsætte krav til bl.a. kompleksiteten og længden af adgangskoder, og hvor ofte de skal skiftes. Alt efter karakteren af de oplysninger en organisation behandler, kan det være nødvendigt at beskytte adgangen til personoplysninger ved at stille krav til brugernes valg af adgangskoder. Organisationen vil i tilknytning hertil også skulle indrette tekniske systemadgange på en sådan måde, at brugere ikke kan oprette koder, som ikke lever op til de fastsatte krav. Mere information og gode råd til oprettelse af stærke adgangskoder kan findes her: https://sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed/6-lav-staerke-adgangskoder/ https://cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/-vejledning-passwordsikkerhed-2020.pdf **Henvisninger** ISO 27001 – A.9.4.2 ISO 27002 – 9.4.2
5.3	Har organisationen implementeret to-faktor-autentifikation ved adgang til systemer og databaser,	**Hjælpetekst** Med 'to-faktor-autentifikation' menes en login-proces, som indebærer to godkendelseselementer. Man taler typisk om, at et sådant godkendelseselement er:

	hvor der opbevares og behandles personoplysninger?	• ”Noget man ved” (f.eks.et brugernavn i kombination en adgangskode), • ”Noget man har” (f.eks. et nøglekort eller en pc, som – via et på forhånd installeret certifikat – kan genkendes af den it-løsning, som brugeren forsøger at tilgå) og • ”Noget man er” (f.eks. et fingeraftryk eller en iris-skanning). Det er kombinationen af to af disse elementer, der udgør de to faktorer. Et eksempel kunne være en online-baseret betalingsløsning, hvor brugeren skal indtaste brugernavn/adgangskode (”noget man ved”) i kombination med sms-engangskode, som modtages på brugerens mobiltelefon (”noget man har”). Et andet eksempel kunne være et sagsbehandlingssystem i en virksomhed, som kan tilgås via internettet, og hvor brugeren både skal indtaste brugernavn/adgangskode (”noget man ved”) og anvende sin arbejds-pc med godkendt certifikat (”noget man har”). Hvis oplysningerne derimod opbevares på selve pc’en, og denne pc alene er beskyttet med brugernavn/adgangskode, er der IKKE tale om to faktorer – heller ikke selv om man både skal have pc’en i sin besiddelse og kende brugernavn/adgangskode. **Henvisninger** ISO 27001 – A.9.4 ISO 27002 – 9.4
5.4	Foretager organisationen regelmæssigt en dokumenteret kontrol af medarbejdernes adgangsrettigheder for at sikre at tildelte brugeradgange og rettigheder er korrekte?	**Hjælpetekst** Det er ikke tilstrækkeligt kun at have styr på, hvilke adgangsrettigheder nye brugere skal have. Organisationer vil også kunne opleve, at brugernes behov for at kunne tilgå oplysninger ændrer sig med tiden, f.eks. ved ændringer eller ophør af ansættelsesforhold. Derfor skal organisationen løbende sikre sig, at adgangsrettigheder til personoplysninger løbende tilpasses efter brugernes faktiske behov. Med ’regelmæssigt’ menes periodiske intervaller, som er passende for organisationen – typisk hvert kvartal eller hvert halvår. Intervallet kan dog være afhængigt af f.eks. kompleksiteten af organisationen eller større organisatoriske, fysiske og it-mæssige ændringer. **Henvisninger** ISO 27001 – A.9.2 ISO 27002 – 9.2
5.5	Foretager organisationen automatisk registrering af medarbejdernes aktiviteter i it-systemer, som anvendes til behandling af personoplysninger (logoversigt)?	**Hjælpetekst** En sådan automatisk registrering betegnes også som ’logning’. Logning er et vigtigt redskab til at kortlægge, f.eks. hvordan brugere af et it-system har ageret. Logningen/registreringerne af brugernes adfærd gengives i en såkaldt logoversigt eller logfil, som efterfølgende kan anvendes til bl.a. at analysere og dokumentere eventuelt misbrug af oplysninger.

		Logning kan i øvrigt også være et vigtigt værktøj til at opdage eventuelle hackere eller andre uvedkommendes adgang til organisationens systemer. **Henvisninger** ISO 27001 - A.12.4 ISO 27001 - A.6.1.2 ISO 27002 - 12.4 ISO 27002 - 6.1.2
5.6	Foretager organisationen regelmæssigt en gennemgang af logoversigter for at identificere usædvanlige hændelser og uautoriseret adgang?	**Hjælpetekst** Selvom brugere (f.eks. medarbejdere) har fået tildelt brugeradgang/rettigheder til et it-system, er det ikke ensbetydende med, at de frit kan anvende personoplysninger. For at opdage et eventuelt misbrug af oplysninger, kan det være nødvendigt løbende - eller med mellemrum - at foretage en eller anden form for kontrol af brugernes adfærd. En sådan kontrol kan også virke præventivt, hvis brugerne er klar over, at et eventuelt misbrug vil kunne opdages. Med 'regelmæssigt' menes periodiske intervaller, som er passende for organisationen – typisk ugentligt eller hver måned eller ved allarmering om et usædvanlig adfærd. Intervallet kan dog f.eks. være afhængigt af, hvor kritisk et it-system er, kompleksiteten af organisationen og den omskiftende risikobillede. **Henvisninger** ISO 27001 - A.12.4.2 ISO 27002 - 12.4.2
6.	**Medarbejdernes øvrige brug af it**	
6.1	Fører organisationen en skriftlig oversigt over alle de digitale værktøjer (programmer og elektronisk udstyr), som medarbejdere bruger i deres arbejde?	**Hjælpetekst** Med 'oversigt' menes et dokument, som identificerer de aktiver (programmer og elektronisk udstyr), og som anvendes til behandling af bl.a. personoplysninger. En sådan oversigt kan være et vigtigt værktøj til at holde styr på, hvor organisationens personoplysninger behandles således, at man kan beskytte oplysningerne på den mest hensigtsmæssige måde, herunder at man også kan sikre sig, at oplysningerne slettes, når man ikke længere skal bruge dem. **Henvisninger** ISO 276001 - A.8.1.1 ISO 27002 - 8.1.1
6.2	Har organisationen begrænset medarbejderenes rettigheder til at installere programmer mv. ned til deres computere og mobile enheder?	**Hjælpetekst** Begrænsning af rettigheder indebærer en teknisk opsætning, som begrænser medarbejdernes muligheder for at installere ikke-godkendt software og applikationer.

		Alt efter organisationens størrelse og kompleksitet kan det være nødvendigt at begrænse medarbejdernes rettigheder til at hente og installere programmer på deres arbejdsudstyr. En sådan begrænsning kan bl.a. bidrage til beskyttelse mod cybersikkerhedstrusler, som bl.a. kan ramme organisationen gennem download af tvivlsomme programmer af ukendt oprindelse (malware, virus mv.) eller gennem den efterfølgende brug programmerne, som ikke løbende bliver sikkerhedsopdateret på grund af organisationens manglende kendskab til dem (f.eks. sikkerhedshuller pga. manglende patching). **Henvisninger** ISO 27001 - A.8.1.3 ISO 27002 - 8.1.3
6.3	Uddanner organisationen løbende medarbejdere i it-sikkerhed og sikker behandling af personoplysninger?	**Hjælpetekst** Med 'uddanner' menes interne eller eksterne kurser om sikkerhed på arbejdspladsen og om behandling af personoplysninger, som er relevante for medarbejdernes løsning af arbejdsopgaver og deres generelle adfærd. Sådan en uddannelse, ofte kaldt awareness-træning, kan også bestå af interne oplæg, møder og workshops, hvor forsvarlig adfærd og relevante scenarier drøftes. Det kan typisk være relevant at gennemføre awareness-træning for nye medarbejdere som en del af deres introduktion. Alt efter organisationens størrelse og kompleksitet - og ved større organisatoriske ændringer - kan det være nødvendigt at afholde løbende awareness-træning, så medarbejderne kan holde sig ajour med organisationens politikker og retningslinjer i det omfang, det er relevant for deres jobfunktion. Mere information om medarbejderes awareness-træning kan findes her: https://sikkerdigital.dk/virksomhed/beskyt-virksomheden/medarbejderpakken/ https://owasp.org/www-project-top-ten/2017/Top_10.html **Henvisninger** ISO 27001 - A.7.2.2 ISO 27002 - 7.2.2
7.	**Netværkssikkerhed og transport**	
7.1	Anvender organisationen ét eller flere sikkerhedsprogrammer, f.eks. antivirus, antispyware, antiphishing og sårbarhedsscanner, som løbende bliver opdateret?	**Hjælpetekst** I et højt digitaliseret samfund, hvor truslen fra f.eks. cyberkriminelle er meget høj, er det vigtigt, at organisationen har forholdt sig til risikoen for cyberangreb som for eksempel ransomware. Dette vil ofte betyde, at der skal installeres sikkerhedsprogrammer på servere og medarbejdernes computere og servere. Alt efter organisationens aktiviteter kan det være nødvendigt at overveje, om andre enheder skal beskyttes mod cybertrusler. Det kan være computere, som er offentligt tilgængelige (f.eks. på biblioteker og borgercentre) eller delt mellem flere medarbejdere (f.eks. en delt pc på et værksted eller i en butik). Hertil kommer, at smartphones og tablets i stadig højere grad anvendes af organisationer til kommunikation og udveksling af oplysninger på lige fod med computere, og derfor kan behovet for beskyttelse med sikkerhedsprogrammer også være relevant i denne sammenhæng.

		Med 'sikkerhedsprogrammer' menes software, som installeres på organisationens it-udstyr og mobile enheder, og som har til formål at forebygge uvedkommendes adgang til it-systemer og personoplysninger. Dette spørgsmål (7.1) omfatter ikke firewalls, som er omfattet af spørgsmål 7.2. Med 'løbende opdateret' menes, at organisationen har etableret en proces, som understøtter, at de seneste versioner af sikkerhedsprogrammerne altid er installeret. Mere information om relevante sikkerhedstiltag kar findes her: https://cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/-reducer-risikoen-for-falske-mails-2018.pdf https://startvaekst.virk.dk/node/1884/security-report/recommendations/pdf **Henvisninger** ISO 27001 - A.12.2.1 ISO 27002 - 12.2.1
7.2	Har organisationen etableret egne særskilte firewalls for at beskytte it-udstyr, systemer og databaser, der anvendes til at behandle personoplysninger?	**Hjælpetekst** Med 'firewall' menes en digital barriere mellem organisationens eget netværk og andre netværk. En sådan firewall overvåger indgående og udgående netværkstrafik og blokerer for uønsket data baseret på allerede opsatte sikkerhedsregler. En firewall kan både være software- og hardwarebaseret. **Henvisninger** ISO 27001 - A.13.1 ISO 27002 - 13.1
7.3	Har organisationen segmenteret (adskilt) egne netværk?	**Hjælpetekst** Ved at segmentere/adskille netværk kan organisationen begrænse skaden ved f.eks. hackerangreb eller malware. Alt efter organisationens størrelse, kompleksitet og typer af behandlingsaktiviteter kan det være nødvendigt at overveje om opdeling af netværk skal ske på baggrund af tillidsniveauer (f.eks. offentligt domæne, pc-domæne, serverdomæne), på baggrund af organisatoriske enheder (f.eks. HR, økonomi, marketing) eller en kombination af begge (f.eks. serverdomæne koblet til flere organisatoriske enheder). Med 'segmenteret (adskilt)' menes, at organisationen har opdelt sin netværksinfrastruktur i to eller flere separate netværk typisk adskilt af en firewall. **Henvisninger** ISO 27001 - A.13.1 ISO 27002 - 13.1
7.4	Har organisationen implementeret kryptering af harddisk og/eller filsystem på medarbejdernes bærbare computere?	**Hjælpetekst** Kryptering er en sikkerhedsforanstaltning, som bl.a. beskytter oplysninger mod uvedkommende adgang. Med 'kryptering af harddisk og/eller filsystem' menes en software- eller hardwarebaseret krypteringsløsning, der sikrer, at indholdet er krypteret før indtastning af brugerens password. Ved harddisk kryptering (full disk encryption) er harddiskens indhold altid

		krypteret, og kun dele dekrypteres og placeres i hukommelsen (RAM) ved brug. Ved kryptering af filsystemet sikres indholdet af hele/dele af filsystemet, men ikke selve operativsystemet/systemfiler, mv. Eksempler på kendte software løsninger er BitLocker (Microsoft), FileVault (Apple), LUKS (Linux) eller VeraCrypt (IDRIX). **Henvisninger** Databeskyttelsesforordningens artikel 25
7.5	Krypterer organisationen fortrolige og følsomme personoplysninger ved overførsel (transport) via internettet, f.eks. via HTTPS eller FTPS, og/eller med e-mail?	**Hjælpetekst** Når oplysninger sendes over åbne netværk som f.eks. internettet, har man som afsender eller modtager som udgangspunkt ingen kontrol over, hvilke maskiner (servere m.v.) de konkrete oplysninger passerer igennem undervejs, herunder hvor i verden disse maskiner er lokaliseret. For at sikre sig mod, at de overførte oplysninger tilgås af uvedkommende, kan man anvende kryptering. Med 'overførsel' menes ikke kun transmission af oplysninger med e-mails, men også anden form for transmission af personoplysninger over netværk, som organisationen ikke har fuld kontrol over. Mere information om typer digital svindel kan findes her: https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed-/transmission-af-personoplysninger/transmission-af-personoplysninger-via-e-mail https://sikkerdigital.dk/myndighed/databeskyttelse-og-gdpr/indbygget-databeskyttelse/ https://sikkerdigital.dk/borger/digital-svindel/ **Henvisninger** Databeskyttelsesforordningens artikel 25 ISO 27001 – A.10.1 ISO 27001 - A.14.1 ISO 27002 – 10.1 ISO 27002 - 14.1
8.	**Patching og backup**	
8.1	Har organisationen etableret en proces for regelmæssigt at opdatere i programmer, styresystemer og andre softwareløsninger (patching)?	**Hjælpetekst** En patch er en opdatering til et computerprogram, og i nogle tilfælde har patching til formål at lukke såkaldte sikkerhedshuller i programmer. Løbende patching er således et væsentligt element i håndteringen af it-sikkerheden hos en organisation. Med 'proces' menes, at enten ledelsen – eller medarbejdere bemyndiget hertil – aktivt har forholdt sig til og tilkendegivet, hvilken software der skal patches, hvor ofte og hvordan dette i praksis skal ske. En sådan stillingtagen kan f.eks. være kommet til udtryk i interne politikker, procesbeskrivelser, informationssikkerhedsdokumenter (f.eks. en Statement of Applicability - SOA), mødereferater og kontrakter med underleverandører.

		Henvisninger Databeskyttelsesforordningens artikel 5, stk. 1, litra e og artikel 32, stk. 1, litra b og c. ISO 27001 - A.12.3.1 ISO 27002 - 12.3.1 ISO 27701 - 6.9.3
8.2	Tager organisationen backup af data og personoplysninger med regelmæssige mellemrum?	**Hjælpetekst** Med 'backup' menes en kopi af organisationens data således, at organisationen til enhver tid har en (forholdsvis opdateret) kopi af sine data til rådighed – de aktuelt anvendte data, der opdateres løbende, samt backup-kopien, der er et historisk øjebliksbillede. Jo længere tid, der går mellem, at organisationen opretter og gemmer en backup-kopi af sine data, desto større forskel vil der normalt være mellem de aktuelt anvendte data og den seneste backup-kopi. Med 'regelmæssige mellemrum' menes, at der tages backup med intervaller, som er passende for den pågældende organisation (bl.a. under hensyn til, hvor vigtige informationerne er for organisationen og/eller kunderne). Det kan typisk være relevant at tage fuld eller delvis backup på timebasis, dagligt eller ugentligt. Backup-kopien bør opbevares adskilt fra de aktuelt anvendte data og skal sikre, at organisationen kan genetablere it-driften, hvis de aktuelt anvendte data går tabt eller bliver beskadiget. Dette kunne f.eks. være relevant, hvis hackere har udnyttet en sårbarhed hos organisationen og krypteret oplysninger. Yderligere information og gode råd til en robust backup-løsning kan findes på: https://sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed/4-tag-backup-af-data **Henvisninger** Databeskyttelsesforordningens artikel 32, stk. 1, litra b, c. ISO 27001 - A.12.3.1 ISO 27002 - 12.3.1 ISO 27701 - 6.9.3
8.3	Har organisationen inden for det seneste år testet, hvorvidt backup data kan genindlæses (reetableres) for at forebygge datatab, for eksempel i tilfælde af ransomware angreb eller nedbrud i it-systemerne?	**Hjælpetekst** Mangelfuld eller fejlet backup er en af de mere almindelige årsager til, at virksomheder mister deres data. Mange organisationer opdager først for sent, at deres backup ikke fungerer. Derfor bør organisationen kontrollere, at en eventuelt backup-løsning fungerer, som den skal. Ved test af backup-løsninger spørges der til, om organisationen i praksis har kontrolleret • hvorvidt der tages backup i overensstemmelse med de forudsatte tidsintervaller (hyppighed), • hvorvidt backup-kopien indeholder alle relevante data (omfang), • hvorvidt backup-kopien er retvisende (integritet), og • hvorvidt de opgældende data rent faktisk kan genindlæses som forudsat (restore).

		Henvisninger ISO 27001 - A.12.3.1 ISO 27002 - 12.3.1 ISO 27701 - 6.9.3
9.	**Behandling af personoplysninger**	
9.1	Har organisationen taget udtrykkelig stilling til, hvornår personoplysninger skal slettes?	**Hjælpetekst** En organisation skal sikre sig, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles. Det vil med andre ord sige, at man ikke må behandle personoplysninger længere end nødvendigt. Herefter skal oplysninger slettes. Med 'sletning' forstås en handling, der medfører, at personoplysninger fjernes fra it-systemer, cloud-løsninger, fysiske papirdokumenter og evt. lokale opbevaringer på medarbejdernes aktiver (PC'er, mobiltelefoner, tablets, USB, eksterne harddiske, e-mail) således, at det ikke længere er muligt at tilgå eller genskabe oplysningerne. For en god ordens skyld skal det også nævnes, at en effektiv anonymisering af personoplysninger kan sidestilles med sletning. Med 'taget udtrykkelig stilling' menes, at f.eks. ledelsen (eller en af ledelsen udpeget ansvarlig person) har forholdt sig til spørgsmålet om, hvornår oplysninger skal slettes, og at dette er kommet til udtryk på skrift, f.eks. i en slettepolitik, en oversigt over slettefrister eller et mødereferat. Mere om krav til sletning af personoplysninger kan findes her: https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed-/sletning https://sikkerdigital.dk/myndighed/databeskyttelse-og-gdpr/sletning-af-personoplysninger/ **Henvisninger** Databeskyttelsesforordningens artikel 5, stk. 1, litra e
9.2	Har organisationen indført faste procedurer/rutiner for rutinemæssig sletning af personoplysninger?	**Hjælpetekst** Som organisation (dataansvarlig) bør man sikre sig, at der er taget stilling til, hvilke procedurer der skal følges, når personoplysninger skal slettes. En sletteprocedure bør normalt dække over de skridt, der skal gennemføre fra det tidspunkt, hvor en personoplysning, når sin slettefrist, til sletningen er foretaget og bekræftet. Indførelsen af sletteprocedurer skal sikre, at organisationen kun opbevarer og behandler personoplysninger, som er nødvendige. Mere om krav til sletning af personoplysninger kan findes her: https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed-/sletning **Henvisninger** Databeskyttelsesforordningens artikel 5, stk. 1, litra e

9.3	Har organisationen taget udtrykkeligt stilling til anvendelse af personoplysninger i forbindelse med eventuel udvikling af programmer, f.eks. ved test af nye programmer eller ændringer i eksisterende programmer?	**Hjælpetekst** Som udgangspunkt bør man ikke anvende "rigtige" personoplysninger i forbindelse med udvikling af programmer, herunder i testmiljøer. I nogle tilfælde kan det dog være nødvendigt at bruge personoplysninger i testsammenhæng for at sikre sig, at systemet virker efter hensigten. Med 'taget udtrykkelig stilling' menes, at f.eks. ledelsen (eller en af ledelsen udpeget ansvarlig person) har forholdt sig til spørgsmålet om, hvornår og hvordan der må anvendes personoplysninger i forbindelsen med udvikling af programmer, og at dette er kommet til udtryk på skrift, f.eks. i en politik, en instruks eller et mødereferat.
9.4	Har organisationen skriftlige retningslinjer om håndtering af anmodninger om indsigt i personoplysninger?	**Hjælpetekst** En person (den registrerede) har ret til at få at vide, om en dataansvarlig behandler oplysninger om den pågældende, herunder bl.a. hvilke oplysninger det drejer sig om, og hvad formålene med behandlingen er. Den dataansvarlige skal i den forbindelse udlevere en kopi af de personoplysninger, der behandles. Denne rettighed kaldes "Den registreredes indsigtsret" og følger af databeskyttelsesforordningens artikel 15. Alt efter organisationens størrelse og kompleksitet kan det være nødvendigt at udarbejde en formaliseret proces for håndtering af sådanne anmodninger fra de registrerede. En proces vil typisk beskrive ansvarsfordelingen internt i organisationen, og hvordan anmodninger i praksis skal imødekommes. Sådanne retningslinjer kan være med til at sikre, at alle registrerede får svar på deres anmodninger, og at organisationen overholder sin forpligtelse i henhold til forordningen. Mere om de registreredes rettigheder og krav til efterlevelse af indsigtsanmodninger kan findes her: https://www.datatilsynet.dk/Media/C/0/Registreredes%20rettigheder.pdf **Henvisninger** Databeskyttelsesforordningens artikel 15.
9.5	Gennemfører organisationen regelmæssig scanning af hjemmesider for utilsigtet offentliggørelse af personoplysninger?	**Hjælpetekst** Utilsigtet offentliggørelse af personoplysninger på hjemmesider er en relativt almindelig hændelse, og det kan – alt efter karakteren af en organisation – være nødvendigt at implementere særlige foranstaltninger for at sikre sig mod sådanne fejl. Med 'scanning' menes en (løbende eller regelmæssig) automatiseret monitorering/overvågning af organisationens hjemmesider for udvalgte personoplysninger, f.eks. personnumre eller andre personoplysninger, hvor der for organisationen er nærliggende risiko for en utilsigtet offentliggørelse. **Henvisninger** Databeskyttelsesforordningens artikel 32.
9.6	Foretager organisationen scanning af udgående e-mails for at undgå utilsigtet forsendelse af personoplysninger?	**Hjælpetekst** Det forekommer desværre relativt ofte, at der ved udsendelse af e-mails sker menneskelig fejl med håndteringen af personoplysninger. Det sker typisk ved, at man sender de "rigtige" personoplysninger til en "forkert" e-mail-adresse, eller ved at man vedhæfter et dokument med "forkerte" personoplysninger til den "rigtige" e-mail-adresse. Alt efter karakteren af

		forseelsen vil det være nødvendigt for en organisation at implementere særlige foranstaltninger for at sikre sig mod sådanne fejl. Med 'scanning' menes en (løbende) automatiseret monitorering af udgående e-mails for udvalgte personoplysninger, f.eks. personnumre eller andre relevante personoplysninger. **Henvisninger** Databeskyttelsesforordningens artikel 32.
10.	**Håndtering af brud på persondatasikkerheden**	
10.1	Har organisationen udpeget en ansvarlig for at anmelde brud på persondatasikkerheden?	**Hjælpetekst** Ved 'ansvarlig' spørges der til, om der udtrykkeligt er udpeget én eller flere bestemt(e) person(er) eller én bestemt afdeling som har ansvaret for at anmelde brud på persondatasikkerheden til Datatilsynet. Yderligere information kan findes på Datatilsynets hjemmeside: https://www.datatilsynet.dk/sikkerhedsbrud/anmeld-sikkerhedsbrud/ og i Datatilsynets vejledning om håndtering af brud på persondatasikkerhed: https://www.datatilsynet.dk/Media/1/9/haandtering-af-brud-paa-persondatasikkerheden%20(3).pdf **Henvisninger** Databeskyttelsesforordningens artikel 33
10.2	Har organisationen udarbejdet skriftlige retningslinjer for håndtering af brud på persondatasikkerheden?	**Hjælpetekst** Et 'brud på persondatasikkerheden' er typisk en hændelse (et uheld eller ved en bevidst handling), hvor personoplysninger kommer til uvedkommendes kendskab, hvor personoplysninger ikke er tilgængelige eller hvor personoplysninger ikke længere er retvisende. Et sådant brud vil efter omstændighederne kunne medføre en risiko for de personer, som oplysningerne vedrører, og i visse tilfælde skal brud anmeldelses til Datatilsynet. Med 'håndtering' menes en beskrivelse af den arbejdsgang eller de praktiske skridt, der skal gennemføres fra det tidspunkt et brud på persondatasikkerheden opdages og indtil det tidspunkt, hvor der eventuelt skal ske anmeldelse til Datatilsynet. Yderligere information om krav til håndtering af sikkerhedsbrud kan læses i Datatilsynets vejledning her: https://www.datatilsynet.dk/Media/1/9/haandtering-af-brud-paa-persondatasikkerheden%20(3).pdf **Henvisninger** Databeskyttelsesforordningens artikel 4, nr. 12. Databeskyttelsesforordningens artikel 33. ISO 27001 - A.16.1.1

		ISO 27002 - 16.1.1 ISO 27701 - 6.13
10.3	Har organisationen et systematiseret overblik over alle tidligere brud på persondatasikkerheden?	**Hjælpetekst** Et overblik over passerede brud på persondatasikkerheden kan hjælpe organisationen med at vurdere, om gennemførte foranstaltninger har været virkningsfulde. En sådan oversigt kan f.eks. bidrage til en forståelse af, om bestemte typer af brud er tilbagevendende eller sker hyppigere end andre brudtyper. Ved 'systematiseret overblik' forstås et skriftlig dokument, som på overskuelig vis gengiver informationer om brud på persondatasikkerheden – herunder særligt de faktiske omstændigheder ved bruddet på persondatasikkerheden (hvad skete der?), dets virkninger (hvad var konsekvenserne for de berørte personer?) og de trufne afhjælpende foranstaltninger (hvad er der gjort for at rette op på situationen både aktuelt og fremadrettet?). **Henvisninger** Databeskyttelsesforordningens artikel 33, stk. 5.
10.4	Foretager organisationen en regelmæssig gennemgang af tidligere brud på persondatasikkerheden for at vurdere, om særlige typer brud kan undgås i fremtiden?	**Hjælpetekst** Brud på persondatasikkerheden kan være et tegn på, at organisationen ikke i tilstrækkelig grad har forholdt sig til alle de risici, som behandlingen af personoplysninger indebærer, f.eks. fordi risikobilledet har ændret sig. Derfor vil det normalt være nyttigt at gennemgå de tidligere brud for at vurdere, om allerede implementerede tekniske og organisatoriske sikkerhedsforanstaltninger er passende. Med 'vurdere' spørges der til, hvorvidt organisationen analyserer karakteren og hyppigheden af tidligere brud med henblik på at forbygge nye brud – f.eks. gennem intern uddannelse af medarbejdere eller implementering af (yderligere) tekniske foranstaltninger. Med 'regelmæssig gennemgang' menes intervaller, der er passende for organisationen – eksempelvis hvert halve eller hele år. Intervallerne kan dog være afhængig af f.eks. antallet af brud eller større organisatoriske, fysiske og it-mæssige ændringer i organisationen. **Henvisninger** Databeskyttelsesforordningens artikel 32, stk. 1, d ISO 27001 - A.16.1.6 ISO 27001 - A.12.4.1 ISO 27002 - 16.1.6 ISO 27002 - 12.4.1
10.5	Hvor mange brud på persondatasikkerheden har organisationen registreret i det foregående kalenderår?	**Hjælpetekst** Med 'brud' menes alle de hændelser (af varierende alvorlighed), som organisationen har registreret i sin oversigt, herunder også brud som ikke blev anmeldt til Datatilsynet, fordi det var usandsynligt, at bruddet indebar en risiko for de registrerede.

		Yderligere information om anmeldelser af sikkerhedsbrud kan findes i Datatilsynets vejledning her: https://www.datatilsynet.dk/Media/1/9/haandtering-af-brud-paa-persondatasikkerheden%20(3).pdf **Henvisninger** Databeskyttelsesforordningens artikel 33, stk.5.
10.6	Hvor mange af disse brud på persondatasikkerheden fra det foregående kalenderår er blevet anmeldt til Datatilsynet?	**Hjælpetekst** Med 'denne kategori af sikkerhedsbrud' menes der hændelser, som medførte så stor en risiko for de registrerede, at de var påkrævet anmeldelse til Datatilsynet. Yderligere information om krav til anmeldelser af sikkerhedsbrud kan findes i Datatilsynets vejledning: https://www.datatilsynet.dk/Media/1/9/haandtering-af-brud-paa-persondatasikkerheden%20(3).pdf **Henvisninger** Databeskyttelsesforordningens artikel 33.
10.7	Hvor mange af disse brud på persondatasikkerheden førte til underretning af de registrerede?	**Hjælpetekst** Ved 'underretning af de registrerede' forstås en orientering af de berørte registrerede enten direkte eller indirekte (f.eks. ved offentliggørelse på en hjemmeside). Orienteringen til de berørte personer skal være formuleret i et klart og forståeligt sprog og skal bl.a. beskrive karakteren af bruddet. Yderligere information om anmeldelse af sikkerhedsbrud kan findes i Datatilsynets vejledning: https://www.datatilsynet.dk/media/6558/haandtering-af-brud-paa-persondatasikkerheden.pdf **Henvisninger** Databeskyttelsesforordningens artikel 33, stk. 3, b, c og d og artikel 34, stk. 2.
11.	**Beredskab**	
11.1	Har organisationen taget stilling til, hvordan driften af vigtige (kritiske) forretningsopgaver opretholdes helt eller delvis uden it-understøttelse i kortere eller længere tid?	**Hjælpetekster** Mange organisationer forholdt sig til, hvad der skal ske i tilfælde af ulykker, f.eks. brand eller en medarbejder med hjertestop. Det er imidlertid ikke alle organisationer, der har forholdt sig til, hvorvidt det er muligt at opretholde den forretningsmæssige drift, hvis man ikke længere har adgang til vigtige it-systemer. For nogle organisationer vil manglende it-understøttelse være særdeles kritisk, f.eks. for et hospital, hvor andre organisationer er mindre udsatte, f.eks. en genbrugsbutik. For langt de fleste organisationer vil det imidlertid være gavnligt på forhånd at have forholdt sig til disse situationer – selv for genrugsbutikken, hvis salg muligvis vil kunne påvirkes af manglende adgang til elektroniske betalingsløsninger. Med 'hvordan' menes særligt, at der forud for et eventuelt it-nedbrud eller lign. allerede er taget udtrykkeligt stilling til, hvordan og i hvilket omfang medarbejdere i praksis skal udføre deres arbejdsopgaver uden, at den sædvanlige it-understøttelse er til stede. Med 'vigtige (kritiske) forretningsopgaver' menes typisk arbejdsrelaterede opgaver, der er vigtige at udføre for at undgå eller begrænse (større) negative konsekvenser for organisationen og/eller for fysiske personer.

		Eksempler på ovenstående kunne være, at ansvarlige medarbejdere på et plejehjem på forhånd har forholdt sig til, hvordan organisationen sikrer den rigtige udlevering af medicin, hvis organisationen ikke kan tilgå de sædvanlige it-systemer med information om medicinering. Det kan også være at ansvarlige medarbejdere i en virksomhed har taget stilling til, hvordan løn kan udbetales til medarbejderne, hvis lønsystemet er nede, f.eks. ved acontoudbetaling af løn. **Henvisninger** ISO 27002 - 17.1 ISO 27002 - 17.2
11.2	Har organisationen taget stilling til, hvordan it-systemer og it-driften genetableres i tilfælde af nedbrud, f.eks. i tilfælde af hackerangreb, brand, oversvømmelser, tyveri, strømsvigt, sygdom hos nøglemedarbejdere mv.?	**Hjælpetekst** Ligesom det kan være gavnligt på forhånd at forholde sig til, hvordan forretningsaktiviteter helt eller delvis kan drives videre ved manglende it-understøttelse, kan det tilsvarende være gavnligt på forhånd at forholde sig til, hvordan man får genetableret den normale it-drift. Dette indebærer først og fremmest en stillingtagen til ansvars- og rollefordelingen i organisationen, hvis uheldet er ude. Alt efter organisationens karakter kan det også indebære en forudgående kortlægning af bl.a. centrale opgaver og processer, prioritering af ressourcer og systemer samt fastlæggelse af kommunikationskanaler. Med 'taget stilling' menes, at den ansvarlige for genetableringen af it-driften (eller ledelsen) udtrykkeligt har forholdt sig til spørgsmålet om genetablering. Med 'hvordan' menes, at der er taget stilling til processer for genetablering af it-driften – herunder, hvem der skal udføre bestemte opgaver, hvad de pågældende personer i praksis skal gøre, og hvornår eller i hvilken rækkefølge dette skal ske. **Henvisninger** Databeskyttelsesforordningens artikel 32, stk. 1, litra b, c ISO 27001 - A.17.1.2 ISO 27002 - 17.1 ISO 27031 ISO 22301
11.3	Har organisationen udarbejdet en egentligt skriftlig beredskabsplan for håndtering af nedbrud i it-systemer?	**Hjælpetekst** Vejledning fra Beredskabsstyrelsen: https://brs.dk/da/redningsberedskab-myndighed/krisestyring2-og-beredskabsplanlagning/helhedsorienteret-beredskabsplanlagning/beredskabsplaner/ Skabelon til beredskabsplan kan findes her: https://sikkerdigital.dk/media/8750/beredskabsplan.doc
11.4	Foretager Organisationen regelmæssige tests af ovenstående beredskabsplaner og retningslinjer?	**Hjælpetekst** Det kan ske, at nogle elementer i en beredskabsplan ser fornuftigt ud på papiret, men at de i praksis viser sig ikke at fungere som tiltænkt. Sådanne uhensigtsmæssigheder vil man ofte kunne afdække gennem øvelser. Tilsvarende vil sådanne

		øvelser også kunne afdække forhold, som man under udarbejdelsen af beredskabsplanen har overset eller fejlagtigt har vurderet som irrelevante. Med 'regelmæssige' menes et interval, der er passende for organisationen – typisk hvert år eller hvert andet år. Intervallet kan dog være afhængigt af f.eks. kompleksiteten af organisationen og behandlingsaktiviteterne eller større organisatoriske, fysiske og it-mæssige ændringer. Med 'test' menes, at udvalgte scenarier er gennemgået (enten ved en simuleret krisesituation eller ved såkaldte skrivebordsøvelser) med henblik på at træne relevante medarbejdere og identificere eventuelle mangler i planer og procedurer. Information, råd og anbefalinger til test af beredskabsplaner kan bl.a. findes her: https://sikkerdigital.dk/myndighed/iso-27001-implementering/beredskabsstyring/beredskabsspillet/ **Henvisninger** Databeskyttelsesforordningens artikel 32, stk. 1, litra d ISO 27001 - A.17.1.3 ISO 27002 - 17.1.3
12.	**Leverandørforhold**	
12.1	Har organisationen indgået skriftlige leverandøraftaler (databehandleraftaler), som fastsætter krav til et passende sikkerhedsniveau med henblik på beskyttelse af personoplysninger?	**Hjælpetekst** Databeskyttelsesforordningen indeholder en bestemmelse om såkaldte databehandleraftaler. Det er aftaler, der skal indgås, når en organisation vælger at benytte en anden organisation, f.eks. en myndighed eller virksomhed til at behandle personoplysninger på sine vegne. Hvis en privat virksomhed f.eks. bruger en ekstern leverandør til at holde styr på sine kundeinformationer, er det et krav, at de to virksomheder indgår en skriftlig aftale om, hvordan leverandøren må behandle virksomhedens oplysninger. Med 'databehandleraftale' menes et dokument, der lever op til de krav, der er fastsat i databeskyttelsesforordningens artikel 28, og som bl.a. fastlægger, at databehandleren kun må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, at databehandleren iværksætter passende sikkerhedsforanstaltninger, og at databehandleren efter den dataansvarliges valg sletter eller tilbageleverer alle personoplysninger til den dataansvarlige, efter at tjenesterne vedrørende behandlingen er ophørt. Du kan finde Datatilsynets skabelon til databehandleraftale her: https://www.datatilsynet.dk/media/7818/skabelon-til-databehandleraftale-dansk.docx **Henvisninger** Databeskyttelsesforordningens artikel 28

12.2	Har organisationen stillet krav om, at databehandleres behandling af personoplysninger (inklusiv opbevaring) kun må finde sted i EU, på de lokaliteter eller i lande, som er godkendt af den dataansvarlige?	**Hjælpetekst** En databehandleraftale skal som udgangspunkt fastsætte krav om, at databehandleren kun må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder hvorvidt databehandleren kan overføre personoplysninger til et tredjeland eller en international organisation. **Henvisninger** Databeskyttelsesforordningens artikel 28, stk. 3, litra a
12.3	Har organisationen stillet krav om, at databehandlere sletter eller tilbageleverer personoplysninger efter endt behandling?	**Hjælpetekst** Databehandleren skal som udgangspunkt efter den dataansvarliges valg slette eller tilbagelevere alle personoplysninger til den dataansvarlige, efter at tjenesterne vedrørende behandlingen er ophørt, og slette eksisterende kopier. **Henvisninger** Databeskyttelsesforordningens artikel 28, stk. 3, litra g
12.4	Har organisationen stillet krav om, at databehandlere alene må anvende underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af organisationen?	**Hjælpetekst** Databehandleren må ikke gøre brug af en anden databehandler uden forudgående specifik eller generel skriftligt godkendelse fra den dataansvarlige. I tilfælde af generel skriftlig godkendelse skal databehandleren underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer. **Henvisninger** Databeskyttelsesforordningens artikel 28, stk. 2
12.5	Fører organisationen regelmæssigt kontrol med, at databehandlere overholder sine forpligtelser som beskrevet i databehandleraftalen?	**Hjælpetekst** Med 'kontrol' menes, at organisationen (den dataansvarlige) gennem mundtlig eller skriftlig dialog med databehandleren sikrer sig, at databehandleren lever op til kravene i databehandleraftalen. En kontrol kan efter omstændighederne også gennemføres ved et fysisk fremmøde på databehandlerens lokaliteter, hvor organisationen ved selvsyn kan kontrollere f.eks. de fysiske rammer for behandleringen af personoplysninger. En kontrol vil efter omstændighederne også kunne bestå i, at der udarbejdes og gennemgås erklæringer fra uafhængige tredjeparter, f.eks. revisionserklæringer. Med 'regelmæssigt' menes et periodisk interval, der er passende for organisationen – typisk hvert år eller hvert andet år. Intervallet kan dog være afhængigt af f.eks. kompleksiteten af organisationen og behandlingsaktiviteterne eller større organisatoriske, fysiske og it-mæssige ændringer. Du kan finde Datatilsynets vejledende tekst om tilsyn med databehandlere og underdatabehandlere her: https://www.datatilsynet.dk/Media/C/C/Vejledende%20tekst%20om%20tilsyn%20med%20databehandlere%20og%20underdatabehandlere.pdf **Henvisninger** Databeskyttelsesforordningens artikel 28, stk. 3, litra h
13.	**Dokumentation**	

13.1	Kan organisationen inden for tre uger fremsende dokumentation til Datatilsynet for de afgivne svar?	**Hjælpetekst** Dokumentation omfatter politikker, retningslinjer og andre dokumenter, som organisationen i de foregående spørgsmål har tilkendegivet at være i besiddelse af. I spørgsmål 3.4; "Har organisationen udarbejdet en politik for informationssikkerheden ved behandling af personoplysninger?", vil dokumentationen eksempelvis omfatte den omhandlede politik. I en række spørgsmål er der imidlertid ikke spurgt ind til graden af dokumentation eller til specifikke dokumenter. Spørgsmål 7.4; "Har organisationen implementeret kryptering af harddisk og/eller filsystemet på medarbejdernes bærbare computere?" indebærer således ikke i sig selv en stillingtagen til spørgsmålet om dokumentation. Hvis der rent faktisk er sket kryptering af harddiske, vil det imidlertid normalt være muligt at tilvejebringe dokumentation, f.eks. i form af møddereferater, mail-korrespondancer eller udskrevne systemoplysninger. Organisationen bedes ved besvarelsen af nærværende spørgsmål 13.1 tage stilling til, om der i forhold til hvert enkelt af de afgivne svar kan tilvejebringes dokumentation til Datatilsynet inden for en tidsfrist på maksimalt tre uger. På baggrund heraf bedes organisationen vurdere i hvilken grad der kan fremskaffes dokumentation for alle svar eller en delmængde heraf. Datatilsynet vil efter omstændighederne kunne anmode om at få fremsendt dokumentation for en eller flere besvarelser. **Henvisninger** Databeskyttelsesforordningen artikel 58. stk. 1, litra e