DATATILSYNET

SPØRGSMÅL MED HJÆLPETEKSTER

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
1.Aktiviteter				
Aktiviteter		1.1 Hvor mange registrerede behandler organisationen oplysninger om?	Den registrerede er 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 – behandles oplysninger om. Svaret skal angives inden for de mulige intervaller.	Databeskyttelsesforordningens artikel 4, nr. 1

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
Aktiviteter		1.2 Behandler organisationen følsomme personoplysninger om kunder/borgere (særlige kategorier af personoplysninger)?	Følsomme personoplysninger (særlige kategorier af personoplysninger) er udtrykkeligt afgrænset i databeskyttelsesforordningen, og adgangen til at behandle sådanne oplysninger er snævrere end ved almindelige personoplysninger. Følsomme personoplysninger 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	Databeskyttelsesforordningens artikel 9, stk. 1.
Aktiviteter		1.3 Foretager organisationen behandlinger af personoplysninger på andres vegne?	Der tænkes på de situationer/behandlinger af personoplysninger i it-systemer, hvor organisationen stiller disse it-systemer til rådighed for andre virksomheder/myndigheder og dermed, at organisationen er databehandler for andre. Organisationen "ejer" således ikke selv de pågældende personoplysninger og kan alene behandle oplysningerne efter instruks fra den	Databeskyttelsesforordningens artikel 4, nr. 8

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			relevante virksomhed/myndighed. Organisationen kan i sådanne situationer karakteriseres som en såkaldt databehandler.	
2.Organisering og informationssikkerhed				
Organisering og informationssikkerhed		2.1 Har organisationen udpeget en eller flere personer, som er ansvarlig(e) for informationssikkerhed?	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.	ISO 27001:2013 – Anneks A.6.1.1
Organisering og informationssikkerhed		2.2 Følger organisationen én eller flere ledelsesstandarder (f.eks. ISO) for informationssikkerhed?	En standard for informationssikkerhed er normalt et rammeværktøj, som organisationer kan anvende for at sikre, at arbejdet med informationssikkerhed er dækkende. Typisk anvendte informationssikkerhedsstandarder er ISO 2700x Det bemærkes, at adgangen til at se og anvende sådanne standarder typisk vil være forbundet med licens- eller abonnementsomkostninger. Eksempler på standarder kan findes her: https://www.iso.org/isoiec-27001-information-security.html	ISO 27001:2013 – Anneks A.18.2.2
Organisering og informationssikkerhed		2.3 Har organisationen udarbejdet en fortegnelse (oversigt) over alle behandlingsaktiviteter?	En fortegnelse over behandlingsaktiviteter er en skriftlig og elektronisk oversigt, som giver organisationen et overblik over de personoplysninger, som organisationen behandler, herunder formålet med behandlingen, kategorier af oplysninger og registrerede, mv. Yderligere information om krav til fortegnelse kan findes i Datatilsynets	Databeskyttelsesforordningens artikel 30, stk. 1.

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			vejledning her: https://www.datatilsynet.dk/media/6567/fortegnelse.pdf	
Organisering og informationssikkerhed		2.4 Har organisationen udarbejdet en politik for informationssikkerheden ved behandling af personoplysninger?	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 i afsnit 2: https://sikkerdigital.dk/virksomhed/beskyt-virksomheden/saadan-taenker-du-it-sikkerhed-ind-i-forretningen	Databeskyttelsesforordningen artikel 32, stk. 1. ISO 27001:2013 – Anneks A.5.1.1
Organisering og informationssikkerhed		2.5 Følger organisationen et årshjul eller lignende, som sikrer, at alle væsentlige arbejdsgange og dokumenter bliver vedligeholdt, og at alle væsentlige opgaver bliver udført?	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 dette og andre aktiviteter, der skal gennemføres, og fastlægge datoer og ansvar for, at aktiviteterne bliver gennemført. Med 'væsentlige dokumenter' menes dokumenter, som – efter organisationens egen opfattelse – er centrale i forhold til sikringen af informationssikkerheden og databeskyttelsen i organisationen. Med 'væsentlige arbejdsgange' menes arbejdsgange som er vigtige og skal udføres på bestemte tidspunkter eller med bestemte intervaller for, at der kan opretholdes et passendes sikkerhedsniveau. En 'opdatering' indebærer især, at der er taget stilling til eventuelle ændringer i organisationens aktiviteter og struktur, herunder behandlingsaktiviteter og organisationsændringer.	Databeskyttelsesforordningens artikel 32, stk. 1 ISO 27001:2013 – Anneks A.5.1.2 ISO 27001:2013 – Anneks A.6.1.1

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
Organisering og informationssikkerhed		2.6. Bliver alle væsentlige dokumenter – jf. spørgsmål 2.5 – godkendt på ledelsesniveau?	Ledelsen har ansvar for organisationens aktiviteter og behandlinger og bør derfor involvere sig i arbejdet med informationssikkerhed og databeskyttelse. Det kan f.eks. 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 modervselskab.	ISO 27001:2013 – Anneks A.5.1.2 ISO 27001:2013 – Anneks A.18.2.2
3. Risikovurderinger				
Risikovurderinger		3.1 Har organisationen taget udtrykkeligt stilling til, hvordan relevante trusler mod informationssikkerheden vil kunne påvirke organisationens forretningsaktiviteter negativt (en forretningsmæssig risikovurdering)?	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.	ISO 27001:2013 – Afsnit 6.1
Risikovurderinger		3.2 Har organisationen taget udtrykkeligt stilling til, hvordan relevante trusler mod informationssikkerheden vil kunne påvirke de registreredes rettigheder negativt (en databeskyttelsesretlig risikovurdering)?	En 'databeskyttelsesretlig risikovurdering' indebærer, at organisationen tager hensyn til de risici, der er for de registrerede i forbindelse med behandlingen af personoplysninger. 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.	Databeskyttelsesforordningens artikel 32, stk. 2.

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
Risikovurderinger		3.3 Opdateres eventuelle skriftlige risikovurderinger regelmæssigt?	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 ændringer i det generelle risikobillede, 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.	Databeskyttelsesforordningens artikel 32, stk. 1, litra b Databeskyttelsesforordningens artikel 32, stk. 2 ISO 27001:2013 – Afsnit 6.1.2
Risikovurderinger		3.4 Bliver risikovurderinger godkendt på ledelsesniveau?	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	Databeskyttelsesforordningens artikel 32, stk. 2. ISO 27001:2013 – Afsnit 9.3

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			ledelse har forholdt sig til risici og har påtaget sig ansvaret for, at organisationen handler i overensstemmelse med de overvejelser, som fremgår af risikovurderingen.	
4. Adgang til oplysninger				
Adgang til oplysninger		4.1 Har organisationen udarbejdet en skriftlig procedure for at tildele og nedlægge brugeradgange og -rettigheder til it-systemer, når medarbejdere ansættes, ændrer arbejdsopgaver eller fratræder?	Alt efter organisationens størrelse og kompleksitet kan det være nødvendigt at udarbejde en procedure for at administrere brugeres (f.eks. ansattes) systemadgange. En sådan administration af brugeradgange skal være begrundet i brugernes arbejdsbetingede behov og skal passe til formålet med behandlingen af personoplysninger (som angivet i fortegnelsen over behandlingsaktiviteter). Administration af brugeradgange skal forhindre, at brugerne kan tilgå oplysninger, som de ikke har behov for at anvende. Med 'brugeradgange og -rettigheder' menes den opsætning af adgange til it-systemer og it-tjenester, der tildeles brugere, så de kan anvende systemet – ofte efter indtastning af brugernavn og kode.	ISO 27001:2013 – Anneks A.9.2
Adgang til oplysninger		4.2 Foretager organisationen regelmæssigt en dokumenteret kontrol af medarbejdernes adgangsrettigheder for at sikre, at tildelte brugeradgange og rettigheder er korrekte?	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. Her spørges til, om der er en kontrol, som viser, at en sådan tilpasning sker, eller om mange medarbejdere beholder adgange, der skulle være lukket. Med 'regelmæssigt' menes periodiske intervaller. Intervaller kan fx være afpasset til, om man tidligere har oplevet problemer på dette	Databeskyttelsesforordningen artikel 32, stk. 1, litra d. ISO 27001:2013 – Anneks A.9.2.5

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			område eller ej. Det bør også være afpasset til, hvad der skal være mulighed for at undersøge, hvis der har været unødvendige adgange – altså afpasset til hvor langt tilbage der logges på brugernes anvendelser af adgange.	
Adgang til oplysninger		4.3 Foretager organisationen automatisk registrering af medarbejdernes aktiviteter i it-systemer, hvori der sker behandling af personoplysninger (logning)?	Logning er et vigtigt redskab til at kortlægge, f.eks. hvordan brugere af et it-system har ageret. Logning/registrering 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. Om organisationen foretager en logning, der kan anvendes til et sådant formål, forudsætter imidlertid, at der logges de rigtige informationer (logs kan have mange forskellige formål), og at organisationen har konstateret, at logningen fungerer, at logs kan tolkes korrekt, og at logs er beskyttet imod misbrug (manipulering).	Databeskyttelsesforordningen artikel 32, stk. 1, litra d. ISO 27001:2013 – Anneks A.12.4.1
Adgang til oplysninger		4.4 Foretager organisationen regelmæssigt en gennemgang af eller stikprøve i logfiler for at identificere usædvanlige hændelser?	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 alarmering om en usædvanlig adfærd. Intervallet kan afpasses til, hvor kritisk et it-system er, kompleksiteten af organisationen og det omskiftende risikobillede.	Databeskyttelsesforordningen artikel 32, stk. 1 ISO 27001:2013 – Anneks A.12.4.1

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
5. Medarbejdernes brug af IT				
Medarbejdernes brug af IT		5.1 Fører organisationen en skriftlig oversigt over alle de digitale værktøjer (applikationer og elektronisk udstyr), som medarbejdere bruger i deres arbejde?	Med 'oversigt' menes et dokument, som identificerer de aktiver (applikationer 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 personoplysningerne.	ISO 27001:2013 – Anneks A.8.1.1
Medarbejdernes brug af IT		5.2 Uddanner organisationen løbende medarbejdere i it-sikkerhed og sikker behandling af personoplysninger?	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. Ved udskiftning i medarbejderstab og ved større organisatoriske ændringer kan det være nødvendigt at gentage awareness-træningen, 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:	ISO 27001:2013 – Anneks A.7.2.2

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			https://sikkerdigital.dk/virksomhed/beskyt-virksomheden/medarbejder-pakken/	
6. Netværkssikkerhed				
Netværkssikkerhed		6.1 Har organisationen etableret egne særskilte firewalls for at beskytte it-udstyr, systemer og databaser, der anvendes til at behandle personoplysninger?	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 sikkerhedsregler. En firewall kan både være software- og hardwarebaseret.	Databeskyttelsesforordningen artikel 32, stk. 1. ISO 27001:2013 – Anneks A.13.1.1
Netværkssikkerhed		6.2 Har organisationen segmenteret (adskilt) egne netværk?	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, hvor denne segmentering begrænser muligheden for, at en kompromittering af sikkerheden spreder sig fra ét segment til et andet.	Databeskyttelsesforordningen artikel 32, stk. 1. ISO 27001:2013 – Anneks A.13.1.3
7. Backup				

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
Backup		7.1 Tager organisationen backup af data, der indeholder personoplysninger, med regelmæssige mellemrum?	Med 'backup' menes en kopi af organisationens data således, at organisationen til enhver tid har en (forholdsvis opdateret) kopi af sine data til rådighed. 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, under hensyn til, hvilken risiko det vil udgøre for organisationen og de registrerede, hvis organisationen ikke har adgang til aktuelle data. Backup-kopien bør opbevares fysisk og logisk adskilt fra de aktuelt anvendte data, således at de ikke er udsat for samme risici som fx brand. Backup-kopien gør det muligt sammen med den rette hardware og software at 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 data. 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	Databeskyttelsesforordningens artikel 32, stk. 1, litra c. ISO 27001:2013 – Anneks A.12.3.1
Backup		7.2 Har organisationen inden for det seneste år testet, hvorvidt backup data kan genindlæses (reetableres) for at forebygge datatab, for eksempel i	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	Databeskyttelsesforordningens artikel 32,

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
		tilfælde af ransomware angreb eller nedbrud i it-systemerne?	kontrollere, at en eventuel backup-løsning fungerer, som den skal, og at der er den nødvendige viden/dokumentation/kompetence til at re-etablere it-systemerne med den backup, som er taget. Med test af backup-løsninger, menes 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 pågældende data rent faktisk kan genindlæses som forudsat (restore).	stk. 1, litra c. ISO 27001:2013 – Anneks A.12.3.1
8. Behandling af personoplysninger				
Behandling af personoplysninger		8.1 Har organisationen taget udtrykkelig stilling til, hvornår personoplysninger skal slettes?	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. 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.	

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			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/	
Behandling af personoplysninger		8.2 Har organisationen indført faste procedurer/rutiner for rutinemæssig sletning af personoplysninger?	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 beskrive de skridt, der skal gennemføres fra det tidspunkt, hvor en personoplysning når sin slettefrist, til det tidspunkt hvor 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	Databeskyttelsesforordningens artikel 30 Databeskyttelsesforordningens artikel 5, stk. 1, litra e

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
Behandling af personoplysninger		8.3 Har organisationen taget udtrykkeligt stilling til anvendelse af personoplysninger i forbindelse med eventuel udvikling af it-systemer, f.eks. ved test af nye/ændrede it-systemer?	Som udgangspunkt bør man ikke anvende "rigtige" personoplysninger i forbindelse med udvikling af it-systemer, 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 applikationer, og at dette er kommet til udtryk på skrift, f.eks. i en politik, en instruks eller et mødereferat. Mere om brug af personoplysninger i test kan findes her: https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed-/testdata-brug-af-personoplysninger-ved-udvikling-og-test-af-it-systemer	Databeskyttelsesforordningens artikel 25 ISO 27001:2013 – Anneks A.14.3.1
Behandling af personoplysninger		8.4 Har organisationen skriftlige retningslinjer om håndtering af anmodninger om indsigt i personoplysninger?	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	Databeskyttelsesforordningens artikel 15.

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			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	
Behandling af personoplysninger		8.5 Gennemfører organisationen regelmæssig scanning af sit/sine websted(er)for utilsigtet offentliggørelse af personoplysninger?	Utilsigtet offentliggørelse af personoplysninger via sine websider 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 websider for udvalgte personoplysninger, f.eks. personnumre eller andre personoplysninger, hvor der for organisationen er nærliggende risiko for en utilsigtet offentliggørelse.	Databeskyttelsesforordningens artikel 32, stk. 1, litra d
Behandling af personoplysninger		8.6 Foretager organisationen scanning af udgående e-mails for at undgå utilsigtet forsendelse af personoplysninger?	Det forekommer desværre relativt ofte, at der ved udsendelse af e-mails sker menneskelige fejl med håndteringen af personoplysninger. Det sker typisk ved, at man sender de ”rigtige” personoplysninger til en ”forkert” e-mailadresse, eller ved at man vedhæfter et dokument med ”forkerte” personoplysninger til den ”rigtige” e-mailadresse. Alt efter karakteren af forseelsen vil det være nødvendigt for en organisation at implementere særlige foranstaltninger for at sikre sig mod sådanne fejl.	Databeskyttelsesforordningens artikel 32, stk. 1

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			Med 'scanning' menes en (løbende) automatiseret monitorering af udgående e-mails for udvalgte personoplysninger, f.eks. personnumre eller andre relevante personoplysninger.	
9. Håndtering af brud på persondatasikkerheden				
Håndtering af brud på persondatasikkerheden		9.1 Har organisationen udpeget en ansvarlig for at anmelde brud på persondatasikkerheden?	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/637829342599720760/H%C3%A5ndtering%20af%20brud%20p%C3%A5%20persondatasikkerheden.pdf	Databeskyttelsesforordningens artikel 33, stk. 1
Håndtering af brud på persondatasikkerheden		9.2 Har organisationen udarbejdet skriftlige retningslinjer for håndtering af brud på persondatasikkerheden?	Et 'brud på persondatasikkerheden' er typisk en hændelse (et uheld eller ved en bevidst handling), hvorved personoplysninger kommer til uvedkommendes kendskab, eller bliver utilgængelige eller ophører med at være retvisende. Et sådant brud vil efter omstændighederne kunne medføre en risiko for de personer, som oplysningerne vedrører, og i visse tilfælde skal brud anmeldes til Datatilsynet. Med 'håndtering' menes en beskrivelse af den arbejdsgang eller de praktiske skridt, der skal gennemføres fra det tidspunkt, hvorfra der er mistanke om eller konstateret et brud på persondatasikkerheden og	Databeskyttelsesforordningens artikel 33, stk. 1 ISO 27001:2013 – Anneks A.16.1.1

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			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/637829342599720760/H%C3%A5ndtering%20af%20brud%20p%C3%A5%20persondatasikkerheden.pdf	
Håndtering af brud på persondatasikkerheden		9.3 Har organisationen et systematiseret overblik over alle tidligere brud på persondatasikkerheden?	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?).	Databeskyttelsesforordningens artikel 33, stk. 5
Håndtering af brud på persondatasikkerheden		9.4 Foretager organisationen en regelmæssig gennemgang af tidligere brud på persondatasikkerheden for at vurdere, om særlige typer brud kan undgås i fremtiden?	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.	Databeskyttelsesforordningens artikel 32, stk. 1, litra d ISO 27001:2013 –

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			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.	Anneks A.16.1.6
Håndtering af brud på persondatasikkerheden		9.5 Hvor mange brud på persondatasikkerheden har organisationen registreret i det foregående kalenderår?	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.	Databeskyttelsesforordningens artikel 33, stk. 5
Håndtering af brud på persondatasikkerheden		9.6 Hvor mange af disse brud på persondatasikkerheden fra det foregående kalenderår er blevet anmeldt til Datatilsynet?	Brud på persondatasikkerheden skal anmeldes til Datatilsynet, medmindre det er usandsynligt, at bruddet indebærer en risiko for de registreredes rettigheder. Yderligere information om krav til anmeldelser af sikkerhedsbrud kan findes i Datatilsynets vejledning: https://www.datatilsynet.dk/Media/637829338407422117/haandtering-af-brud-paa-persondatasikkerheden%20(3).pdf	Databeskyttelsesforordningens artikel 33, stk. 5.
Håndtering af brud på		9.7 Hvor mange af disse brud på persondatasikkerheden førte til underretning af de registrerede?	Ved 'underretning af de registrerede' forstås en orientering af de berørte registrerede enten direkte eller indirekte (f.eks. ved offentliggørelse i pressen). Orienteringen til de berørte personer skal være formuleret i et klart og forståeligt sprog og skal bl.a. beskrive karakteren af	Databeskyttelsesforordningens artikel 34

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
persondata-sikkerheden			bruddet, de sandsynlige konsekvenser af bruddet, og foranstaltninger som er truffet for at håndtere bruddet. Yderligere information om anmeldelse af sikkerhedsbrud kan findes i Datatilsynets vejledning: https://www.datatilsynet.dk/Media/637829338407422117/haandtering-af-brud-paa-persondatasikkerheden%20(3).pdf	
10. Beredskab				
Beredskab		10.1 Har organisationen taget stilling til, hvordan driften af vigtige (kritiske) forretningsopgaver opretholdes helt eller delvis uden it-understøttelse i kortere eller længere tid?	Mange organisationer har 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 genbrugsbutikken, 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 lignende 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	Databeskyttelsesforordningens artikel 32, stk. 1, litra b, c ISO 27001:2013 – Anneks A.17.1

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			(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.	
Beredskab		10.2 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.?	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.	Databeskyttelsesforordningens artikel 32, stk. 1, litra b, c ISO 27001:2013 – Anneks A.17.1.1

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
Beredskab		10.3 Har organisationen udarbejdet en egentligt skriftlig beredskabsplan for håndtering af nedbrud i it-systemer?	Vejledning fra Beredskabsstyrelsen: https://brs.dk/da/redningsberedskab-myndighed/krisestyring2-og-beredskabsplanlagning/helhedsorienteret-beredskabsplanlagning/beredskabsplaner/ Skabelon til beredskabsplan kan findes her: https://sikkerdigital.dk/virksomhed/beskyt-virksomheden/saadan-taenker-du-it-sikkerhed-ind-i-forretningen	ISO 27001:2013 – Anneks A.17.1.2
Beredskab		10.4 Foretager organisationen regelmæssige tests af ovenstående beredskabsplaner og retningslinjer?	Det kan ske, at nogle elementer i en beredskabsplan ser fornuftige 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:	Databeskyttelsesforordningens artikel 32, stk. 1, litra d ISO 27001:2013 – Anneks A.17.1.3

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			https://sikkerdigital.dk/myndighed/iso-27001-implementering/beredskabsstyring/beredskabsspillet/	
11. Leverandørforhold				
Leverandørforhold		11.1 Har organisationen indgået skriftlige databehandleraftaler med sine leverandører, hvor disse aftaler fastsætter krav til et passende sikkerhedsniveau med henblik på beskyttelse af personoplysninger?	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	Databeskyttelsesforordningens artikel 28, stk. 1 ISO 27001:2013 – Anneks A.15.1.2

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
Leverandør-forhold		11.2 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?	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.	Databeskyttelsesforordningens artikel 28, stk. 3, litra g
Leverandør-forhold		11.3 Har organisationen stillet krav om, at databehandlere sletter eller tilbageleverer personoplysninger efter endt behandling?	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
Leverandør-forhold		11.4 Har organisationen stillet krav om, at databehandlere alene må anvende underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af organisationen?	Databehandleren må ikke gøre brug af en anden databehandler uden forudgående specifik eller generel skriftlig 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.	Databeskyttelsesforordningens artikel 28, stk. 2
Leverandør-forhold		11.5 Fører organisationen regelmæssigt tilsyn med, at databehandlere overholder sine forpligtelser som beskrevet i databehandleraftalen?	Med 'tilsyn' 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 behandlingen af personoplysninger. En kontrol vil efter omstændighederne også kunne bestå i, at der udarbejdes og gennemgås erklæringer fra uafhængige tredjeparter, f.eks. revisionserklæringer.	Databeskyttelsesforordningens artikel 28, stk. 3, litra h ISO 27001:2013 – Anneks A.15.2.1

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			Med 'regelmæssig' menes et periodisk interval, der er konkret tilpasset den enkelte databehandler. Du kan finde Datatilsynets vejledende tekst om tilsyn med databehandlere og underdatabehandlere her: https://www.datatilsynet.dk/Media/637710957381234368/Datatilsynet_Vejledning%20om%20tilsyn%20med%20databehandlere_oktober-2021.pdf	
12. Databeskyttelse gennem design og gennem standardindstillinger				
Databeskyttelse gennem design og gennem standardindstillinger		12.1 Sørger organisationen for, at it-systemers funktionalitet indrettes til at sikre databeskyttelse gennem design?	Sikkerhedsniveauet i behandlingen af personoplysninger i it-systemet skal bl.a. bygge på en vurdering af de risici, som kan opstå ved behandlingen. Databeskyttelse gennem design indebærer, at behandlingen er gennemsigtig, lovlig, rimelig og begrænset til formålet, hvortil personoplysningerne er indsamlet. Datas fortrolighed og tilgængelighed er beskyttet. Data er tilstrækkeligt korrekte/aktuelle til, at behandlingen ikke medfører unødige risici for de registrerede. Endeligt er det sikret, at behandlingen kan ophøre, når den skal (altså at personoplysninger slettes). Du kan læse mere om databeskyttelse gennem design her: https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed-/behandlingssikkerhed-og-databeskyttelse-gennem-design-og-standardindstillinger	Databeskyttelsesforordningens artikel 25, stk. 1 ISO 27001:2013 – Anneks A.14.1

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			og her: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_da.pdf	
Databeskyttelse gennem design og gennem standardindstillinger		12.2 Sørger organisationen for, at som standard behandles kun personoplysninger, der er nødvendige for hvert specifikt formål med behandlingen?	Med udtrykket "som standard" menes at vælge konfigurationsværdier eller databehandlingsmetoder, som er fastlagt eller foreskrevet i et behandlingssystem, f.eks. en softwareapplikation, -tjeneste eller -anordning, eller en manuel behandlingsprocedure, der berører mængden af indsamlede personoplysninger, omfanget af deres behandling, deres opbevaringsperiode og deres tilgængelighed. Du kan læse mere om databeskyttelse gennem standardindstillinger her: https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed-/behandlingssikkerhed-og-databeskyttelse-gennem-design-og-standardindstillinger og her: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_da.pdf	Databeskyttelsesforordningens artikel 25, stk. 2
Databeskyttelse gennem design og gennem standardindstillinger		12.3 Sørger organisationen for, at indkøb, udvikling og ændring af it-systemer sker med baggrund i skriftlige krav/aftaler med leverandører, hvor disse krav/aftaler sikrer et passende sikkerhedsniveau med henblik på beskyttelse af personoplysninger?	En leverandør kan kun forventes at levere det, som er krævet i en skriftlig aftale, og dermed skal krav til behandlingssikkerhed fremgå af aftalen. Aftalen skal med andre ord indeholde mere end blot krav til ønsket funktionalitet i et it-system.	Databeskyttelsesforordningens artikel 25 Databeskyttelsesforordningens artikel 28, stk. 3 (hvis

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			Aftalen skal sikre, at den behandling af personoplysninger, som skal ske i it-systemet, kan ske med et passende sikkerhedsniveau, samt at behandlingen kan ophøre, når den skal. Ved indkøb af eksisterende it-systemer ("hyldevare") skal det sikres, at systemerne i udgangspunktet eller efter tilpasning (og inden ibrugtagning) kan behandle personoplysninger med et passende sikkerhedsniveau, samt at behandlingen kan ophøre, når den skal.	leverandøren er databehandler ift. leverancen) Databeskyttelsesforordningens artikel 32, stk. 1, litra b ISO 27001:2013 – Anneks A.14.1.1 ISO 27001:2013 – Anneks A.15.1.2
Databeskyttelse gennem design og gennem standardindstillinger		12.4 Sørger organisationen for, at it-systemer og tilknyttede manuelle processer testes for, om de beskytter datas fortrolighed, integritet og tilgængelighed?	Både ved ibrugtagning af nye it-systemer og i løbet af deres levetid kan der udføres forskellige tests, som kan sikre, at foranstaltninger vedr. behandlingssikkerhed, fungerer som forventet. Det inkluderer bl.a. test af, om leverandøren har efterlevet krav til behandlingssikkerhed beskrevet i en aftale (spørgsmål 12.3). Det kan også være en del af kontrollen med databehandlerens løbende håndtering af it-systemet, idet driftsmæssige ændringer og ændringer i procedurer kan ødelægge/fjerne sikkerhedsforanstaltninger – uden at der af den grund er sket re-design af it-systemet.	Databeskyttelsesforordningens artikel 25 Databeskyttelsesforordningens artikel 28, stk. 3, litra h Databeskyttelsesforordningens artikel 32, stk. 1, litra d ISO

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
				27001:2013:2013 – Anneks A.14.2.8
13. Konsekvensanalyse				
Konsekvensanalyse		13.1 Har organisationen lavet konsekvensanalyser for alle behandlinger af personoplysninger, der sandsynligvis indebærer en høj risiko for de registrerede?	En konsekvensanalyse er en systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene med behandlingen, herunder i givet fald de legitime interesser, der forfølges af den dataansvarlige. Det inkluderer en vurdering af, om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene. Analysen indeholder desuden en vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder og en beskrivelse af de foranstaltninger, der påtænkes for at imødegå disse risici. Databeskyttelsesforordningens artikel 35, stk. 3, samt følgende liste angiver, hvornår der er påkrævet en konsekvensanalyse, uden dog at udelukke andre omstændigheder: https://www.datatilsynet.dk/Media/4/1/Datatilsynets%20liste%20over%20behandlinger%20der%20altid%20er%20underlagt%20kravet%20om%20en%20konsekvensanalyse%20(2).pdf https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed-/konsekvensanalyse	Databeskyttelsesforordningens artikel 35, stk. 1, 2, 3, 4 og 7
Konsekvensanalyse		13.2 Har organisationen en proces, som sikrer, at ændringer i behandlingsaktiviteter, der har været genstand for en konsekvensanalyse, giver	Der spørges til, hvorvidt organisationen har en proces eller en kontrol til at sikre, at organisationen bliver opmærksom på, at der er sket	Databeskyttelsesforordningens artikel 35, stk. 11

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
		anledning til overvejelser om en fornyet gennemgang af konsekvensanalysen?	en ændring af risikoen for en behandlingsaktivitet, der har været genstand for en konsekvensanalyse. En ændring af risikoen medfører krav om en fornyet gennemgang af konsekvensanalysen, og derfor er det væsentligt, at organisationen er opmærksom på en sådan ændring. https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed-/konsekvensanalyse	
Konsekvensanalyse		13.3 Har organisationen altid inddraget Datatilsynet, når en konsekvensanalyse har vist en høj risiko for de registrerede ved behandlingen af personoplysninger?	Når den dataansvarlige ikke kan finde tilstrækkelige foranstaltninger til at begrænse risiciene til et acceptabelt niveau (dvs. residual-risiciene stadig er høje) skal tilsynsmyndigheden høres, inden behandlingen påbegyndes. https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed-/konsekvensanalyse	Databeskyttelsesforordningens artikel 36, stk. 1
14. Cyber- og informationssikkerhed				
Cyber- og informationssikkerhed	Klienter/pc'er (stationære og bærbare computere der administreres af organisationen)	14.1 Har organisationen en firewall på alle klienter?	Minimumskrav nr. 1 for statslige myndigheder er: *Der skal implementeres firewall på alle klienter.* *Formålet med kravet er at sikre myndighedens klienter mod utilsigtet netværksadgang. Klientbaserede firewalls reducerer risikoen for at en kompromitteret klient kan bruges til at kompromittere andre klienter.* *Kravet er opfyldt, hvis 1) der er implementeret firewall på alle klienter hos myndigheden og 2) myndigheden aktivt har forholdt sig til nødvendig indgående og udgående trafik på klienten og 3)*	Databeskyttelsesforordningens artikel 32, stk. 1 og artikel 5, stk. 1, litra f ISO 27001:2013 – Anneks A.13.1.2

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			firewallpolitikken/konfigureringen kun tillader det, der er identificeret som nødvendigt jf. punkt 2.	
Cyber- og informationssikkerhed	Klienter/pc'er (stationære og bærbare computere der administreres af organisationen)	14.2 Har organisationen på samtlige klienter gennemtvunget anvendelsen af Always On VPN fra eksterne netværk.	Minimumskrav nr. 2 for statslige myndigheder er: *Klienter skal benytte Always On VPN fra eksterne netværk.* *Formålet med kravet er at modvirke man-in-the-middle angreb og sikre, at klientens trafik er omfattet af myndighedens øvrige sikkerhedstiltag. Ved brug af Always On VPN sikres det, at al internettrafik ledes gennem myndighedens egen it-infrastruktur.* *Kravet er opfyldt, hvis 1) der anvendes Always On VPN, når klienten er koblet på netværk uden for myndighedens egen it-infrastruktur og 2) Always On VPN forbindes til myndighedens egen it-infrastruktur, således at al internettrafik går via myndigheden. Tidsbegrænset lokal netværksadgang kan tillades for at kunne anvende login-portaler på fremmed WiFi.*	Databeskyttelsesforordningens artikel 32, stk. 1 og artikel 5, stk. 1, litra f ISO 27001:2013 – Anneks A.9.1.2
Cyber- og informationssikkerhed	Klienter/pc'er (stationære og bærbare computere der administreres af organisationen)	14.3 Har organisationen forhindret, at brugere af bærbare computere (herunder smartphones) uforvarende kan lagre personoplysninger lokalt på enheden, eller er der alternativt implementeret kryptering af harddiske og/eller filsystemer på samtlige computere, hvor det er muligt for brugeren at lagre lokalt?	Minimumskrav nr. 3 for statslige myndigheder er: *Klienters harddiske skal krypteres.* *Formålet med kravet er at undgå kompromittering af data i forbindelse med tab eller tyveri af en klient. Fuld diskkryptering af det lokale faste lager på klienten reducerer risikoen for brud på fortroligheden af data.* *Kravet er opfyldt, hvis der er aktiveret fuld diskkryptering af det lokale faste lager på alle klienter i myndigheden, typisk vha. indbygget funktionalitet i operativsystemet.*	Databeskyttelsesforordningens artikel 25, stk. 2. Databeskyttelsesforordningens artikel 32, stk. 1. ISO 27001:2013 – Anneks A.6.2.2

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			I forhold til ovenstående har Datatilsynet opblødt kravet med et alternativ, hvor man forhindrer, at der placeres personoplysninger på harddiske. Punktet her kan dermed efterleves uden at efterleve minimumskravet på den måde, som statslige myndigheder er forpligtiget til. Kryptering er en sikkerhedsforanstaltning, som bl.a. beskytter oplysninger imod uvedkommendes 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.	ISO 27001:2013 – Anneks A.10.1 ISO 27001:2013 – Anneks A.11.2.6
Cyber- og informationssikkerhed	Klienter/pc'er (stationære og bærbare computere der administreres af organisationen)	14.4 Har organisationen implementeret end-point-beskyttelse mod virus, malware mv. med automatisk opdatering på alle klienter?	Minimumskrav nr. 4 for statslige myndigheder er: *Der skal implementeres endpoint-beskyttelse på alle klienter.* *Formålet med kravet er at opdage og forhindre, at vira og malware mv. afvikles på klienten.* *Kravet er opfyldt, hvis der er installeret endpoint-beskyttelse med automatisk opdatering på alle klienter hos myndigheden.*	Databeskyttelsesforordningens artikel 32, stk. 1, litra b ISO 27001:2013 – Anneks A.12.2.1

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
Cyber- og informationssikkerhed	Klienter/pc'er (stationære og bærbare computere der administreres af organisationen)	14.5 Har organisationen etableret en proces, der sikrer, at alle klienters operativsystemer og applikationer holdes sikkerhesmæssigt opdateret?	Minimumskrav nr. 5 for statslige myndigheder er: *Klienters OS og applikationer på klienten skal holdes sikkerhedsopdateret.* *Formålet med kravet er at lukke kendte sårbarheder på klienterne.* *Kravet er opfyldt, hvis 1) det anvendte operativsystem og applikationerne på klienten er under aktiv support (dvs. der udgives sikkerhedsopdateringer fra producenten) og 2) der er indført tekniske og/eller organisatoriske foranstaltninger, der sikrer at ikke-kritiske systemer opdateres inden for 30 dage, og at kritiske systemer opdateres hurtigst muligt inden da.* En patch er en opdatering til en applikation, og i nogle tilfælde har patching til formål at lukke såkaldte sikkerhedshuller i software. Løbende patching er således et væsentligt element i håndteringen af it-sikkerheden i organisationen. 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 leverandører.	Databeskyttelsesforordningens artikel 32, stk. 1, litra b. ISO 27001:2013 – Anneks A.12.6.1
Cyber- og informationssikkerhed	Klienter/pc'er	14.6 Har organisationen sikret, at almindelige brugerkonti ikke tildeles administrative rettigheder til klienter? Hvis enheden er en smartphone, er der	Minimumskrav nr. 6 for statslige myndigheder er: *Almindelige brugerkonti må ikke tildeles administrative rettigheder til klienter.*	Databeskyttelsesforordningens artikel 32,

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
	(stationære og bærbare computere der administreres af organisationen)	enten samme begrænsning, eller behandlingen af personoplysninger i særlige apps er effektivt beskyttet imod indflydelse fra andre apps på samme enhed.	*Formålet med kravet er at reducere risikoen for installation af malware eller anden kompromittering. Da størstedelen af malware kræver administrative rettigheder på klienten for at blive installeret eller afviklet, må administrative rettigheder ikke tildeles konti, der anvendes til andre aktiviteter.* *Kravet er opfyldt, hvis 1) der er truffet organisatoriske foranstaltninger, med evt. teknisk understøttelse, der sikrer, at administrative rettigheder på klienterne tildeles en separat konto, der kun anvendes til aktiviteter, hvor den administrative rettighed er påkrævet og 2) medarbejdere, hvis primære jobfunktion ikke inkluderer administration af klienter, kun tildeles en separat konto med administrative rettigheder i en tidsbegrænset periode, og på baggrund af en dokumenteret godkendelse af et konkret behov. Ved fornyelse skal en ny godkendelse foretages og dokumenteres.* Spørgsmålet skal også betragtes som omfattende smartphones, hvis disse anvendes som "bærbare computere" til behandling af personoplysninger, som organisationen er dataansvarlig for. "Tidsbegrænsning": En jobfunktion som 'it-supporter' kan udgøre en form for tidsbegrænsning, under den forudsætning, at medarbejderen fratages rettighederne, så snart vedkommende ikke længere besidder jobfunktionen. Begrænsning af rettigheder indebærer en teknisk opsætning, som begrænser medarbejdernes muligheder for at installere (evt. også at	stk. 1 ISO 27001:2013 – Anneks A.6.2.1 ISO 27001:2013 – Anneks A.9.2.3 ISO 27001:2013 – Anneks A.12.6.2

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			hente) ikke-godkendt software. På smartphones kan der alternativt være tale om, at applikationer, der behandler personoplysninger, er så effektivt afskærmet, at de ikke kan påvirkes af installation af ondsindede apps – bemærk dog, at dette ikke løser problemer med, at der fx installeres apps, som kan overtage styringen af mikrofon, kamera, GPS, mv., altså gør telefonen til en overvågningsenhed. Begrænsningen af rettigheder kan bl.a. bidrage til beskyttelse mod cybersikkerhedstrusler, som bl.a. kan ramme organisationen gennem anvendelse af tvivlsomme applikationer af ukendt oprindelse (malware, virus, trojanske heste, mv.), hvor den ondsindede funktion ofte er skjult i software, der umiddelbart har en uskyldig funktion. Endvidere vil sådan software sandsynligvis ikke løbende blive sikkerhedsopdateret, på grund af organisationens manglende kendskab til eksistensen af softwaren.	
Cyber- og informationssikkerhed	Klienter/pc'er (stationære og bærbare computere der administreres af organisationen)	14.7 Har organisationen sikret, at alle pc'er anvender nyeste operativsystem?	Minimumskrav nr. 7 for statslige myndigheder er: *Klienter skal anvende det nyeste operativsystem.* *Formålet med kravet er at sikre, at myndighedens klienter får gavn af de nyeste sikkerhedsfeatures. Da nyere operativsystemer ofte har et højere sikkerhedsniveau end ældre versioner, skal myndigheden anvende det nyeste operativsystem på alle klienter.* *Kravet er opfyldt, hvis det anvendte operativsystem (OS) er en major release eller major update udgivet for mindre end 18 måneder siden.*	Databeskyttelsesforordningens artikel 25 Databeskyttelsesforordningens artikel 32, stk. 1 ISO 27001:2013 – Anneks A.10.1 ISO 27001:2013 – Anneks

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
				A.13.2.3 ISO 27001:2013 – Anneks A.14.1
Cyber- og informationssikkerhed	E-mail (e-mailkommunikation til og fra organisationen)	14.8 Har organisationen sikret, at der kun anvendes godkendte mail-relays med autentifikation?	Minimumskrav nr. 8 for statslige myndigheder er: *Der må kun anvendes godkendte mail-relays med autentifikation.* *Formålet med kravet er at reducere risikoen for misbrug af mail-servere til spredning af malware og spam. Der må derfor kun anvendes mail-relays med autentifikation, som myndigheden har godkendt.* *Kravet er opfyldt, hvis mail-relays, som tilhører eller anvendes af myndigheden, kun accepterer mails fra autentificerede brugere eller systemer. Hvor autentifikation ikke understøttes, skal mail kun accepteres fra positivlistede systemer/software.*	Databeskyttelsesforordningens artikel 32, stk. 1 ISO 27001:2013 – Anneks A.13.2.3
Cyber- og informationssikkerhed	E-mail (e-mailkommunikation til og fra organisationen)	14.9 Har organisationen sikret, at forsendelse af e-mail sendt via internettet eller andre netværk, som ikke er under den dataansvarliges kontrol, altid sker krypteret minimum med TLS 1.2?	Minimumskrav nr. 9 for statslige myndigheder er: *Kommunikation med mail-protokoller skal krypteres og anvende minimum TLS 1.2.* *Formålet med kravet er at kryptere mailtrafikken med henblik på at sikre dataintegritet og fortrolighed. Med anvendelse af TLS 1.2 reduceres risikoen for, at mail-kommunikation bliver aflyttet undervejs i transmissionen over internettet.* *Kravet er opfyldt, hvis 1) alle mail-servere, hvorigennem der kommunikeres til og fra myndigheden er sat op til at kryptere mails med TLS 1.2 såfremt modtager understøtter det (opportunistisk TLS), og 2) alle relevante servere er sat op til at foretage tvungen kryptering (forced TLS)*	Databeskyttelsesforordningens artikel 25 Databeskyttelsesforordningens artikel 32, stk. 1 ISO 27001:2013 – Anneks A.10.1 ISO 27001:2013 –

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			til statslige myndigheder og 3) TLS er konfigureret i henhold til bilag 1 i https://sikkerdigital.dk/Media/637962420328394595/Tekniske%20minimumskrav%20for%20statslige%20myndigheder%202023.pdf Når oplysninger sendes over 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, eller hvem der har adgang til datatransmissionen, herunder hvor i verden maskinerne er lokaliseret. For at sikre sig mod, at de overførte oplysninger tilgås af uvedkommende, kan man anvende kryptering. Bemærk at Datatilsynets spørgsmål også omfatter transmission over andre net end internettet, fx hvis der anvendes MPLS-netværk til udveksling af data mellem fysisk adskilte enheder i en organisation. Information om typer af beskyttelse og 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/	Anneks A.13.2.3 ISO 27001:2013 – Anneks A.14.1

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
Cyber- og informationssikkerhed	Autentifikation	14.10 Har organisationen implementeret to-faktor-autentifikation ved adgang over internettet til it-systemer, og hvor risikovurderingen indikerer et behov for høj sikkerhed?	Minimumskrav nr. 10 for statslige myndigheder er: *Autentifikation til myndighedens systemer over internettet skal anvende flerfaktor-autentificering.* *Formålet med kravet er at reducere risikoen for, at kompromitterede login oplysninger kan anvendes af andre til at tilgå myndighedens systemer og data.* *Kravet er opfyldt, hvis 1) fler-faktor autentifikation er påkrævet ved ekstern adgang til myndighedens data og 2) fler-faktor autentifikationen er baseret på brugerens brugernavn og to eller flere autentifikationstyper. Udstedelse af faktorer baseret på typerne "har" og "er" er baseret på bekræftet identitet eller en anden eksisterende flerfaktor-autentifikation.* En direkte VPN-forbindelse til myndighedens netværk vil også skulle opnås med 2-faktor-autentifikation, for at være tilstrækkelig sikker. Datatilsynet forventer kun dette i situationer, hvor en risikovurdering efter databeskyttelsesforordningens artikel 32, peger på, at der skal en høj sikkerhed til for at etablere et passende sikkerhedsniveau. Dette er fx gældende, hvis der er adgang følsomme/fortrolige personoplysninger. Det kan også være, hvis der fx er adgang til almindelige personoplysninger, men hvor misbrug af adgangen kan ødelægge datas integritet og resultere i alvorlige konsekvenser for de registrerede personer. Med 'to-faktor-autentifikation' menes en login-proces, som indebærer to forskellige hemmelige autentifikationsinformationer, der i	Databeskyttelsesforordningen artikel 32, stk. 1, litra b). ISO 27001:2013 – Anneks A.9.4.2

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			kombinationen beskytter imod risici, som hver autentifikationsinformation isoleret set ville være sårbare overfor. Man taler typisk om, at en sådan autentifikationsinformation er: • ”Noget man ved” (f.eks.et brugernavn i kombination med 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 engangskode fra en kodeviser (”noget man har”). Det er også to-faktor, hvis adgangen kræver fysisk adgang til et netværk i en aflåst bygning (nøglen, eller hvad man nu skal anvende for at komme ind i bygningen, er "noget man har"), kombineret med et login med adgangskode. 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”).	

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
Cyber- og informationssikkerhed	Adgangskoder	14.11 Har organisationen en skriftlig politik for valg af adgangskoder? For mobiltelefoner og lignende er der krav om numerisk adgangskode på min. 6 cifre eller biometrisk identifikation.	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. Spørgsmålet her dækker dels adgangskoder generelt til it-systemer, men også mere specifikke krav for telefoner, tablets og lignende, hvorfra der er adgang til organisationens arbejdsnetværk, og/eller fra hvilke, der kommunikeres på vegne af myndigheden. Bemærk, at den følgende beskrivelse af Minimumskrav nr. 11 kun omhandler mobiltelefoner, tablets og lignende, og er dermed mere begrænset end Datatilsynets spørgsmål. Minimumskrav nr. 11 for statslige myndigheder: *Anvend numerisk adgangskode på minimum 6 cifre eller biometrisk identifikation.* *Formålet med kravet er at beskytte den mobile enhed mod misbrug, hvis den fx tabes eller stjæles.*. 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	Databeskyttelsesforordningens artikel 32, stk. 1 ISO 27001:2013 – Anneks A.9.4.2

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
Cyber- og informationssikkerhed	Mobile enheder (mobiltelefoner og tablets med app-baseret adgang til myndighedens data)	14.12 Har organisationen implementeret MDM (Mobile Device Management) på alle mobile enheder?	Minimumskrav nr. 12 for statslige myndigheder er: *MDM (Mobile Device Management) skal implementeres på alle mobile enheder.* *Formålet med kravet er at beskytte myndighedens data på mobile enheder med særlige sikkerhedstiltag.* *Kravet er opfyldt, hvis MDM-løsningen: 1) sikrer, at de apps der må tilgå myndighedens data, leveres som 'managed apps' og 2) sikrer, at myndighedens data holdes adskilt fra øvrige data og 3) er i stand til at slette myndighedens data på enheden i tilfælde af bortkomst og 4) sletter myndighedens data automatisk ved maksimalt 10 fejlslagne loginforsøg og 5) afviser mobile enheder, der er rooted/jailbroken.*	Databeskyttelsesforordningens artikel 32, stk. 1 ISO 27001:2013 – Anneks A.6.2.1 ISO 27001:2013 – Anneks A.11.2.6
Cyber- og informationssikkerhed	Mobile enheder (mobiltelefoner og tablets med app-baseret adgang til myndighedens data)	14.13 Har organisationen sikret, at operativsystemer og apps på mobile enheder så vidt muligt er opdateret, så snart leverandøren udgiver opdateringer?	Minimumskrav nr. 13 for statslige myndigheder er: *Operativsystem og apps på mobile enheder skal holdes sikkerhedsopdateret.* *Formålet med kravet er at sikre, at kendte sikkerhedshuller lukkes hurtigst muligt. Regelmæssig opdatering sikrer også, at myndighedens mobile enheder får gavn af de nyeste sikkerhedsfeatures.* *Kravet er opfyldt, hvis 1) operativsystemet er under aktiv support (dvs. der udgives sikkerhedsopdateringer) og 2) seneste sikkerhedsopdateringer for operativsystem og 'managed apps' er installeret senest 30 dage efter udgivelse og 3) den mobile enhed er sat op til automatisk opdatering af alle installerede apps.*	Databeskyttelsesforordningens artikel 32, stk. 1, litra d ISO 27001:2013 – Anneks A.6.2.1
Cyber- og informationssikkerhed	Logning	14.14 Har organisationen sikret en logning fra alle it-systemer og tjenester på netværksservere, som gør det muligt at opdage og efterforske	Minimumskrav nr. 14 for statslige myndigheder er: *Krav om logning, log på alle systemer og tjenester på netværksservere.*	Databeskyttelsesforordningens artikel 32,

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
		sikkerhedshændelser, samt sikret at denne log opbevares længe nok?	*Formålet med kravet er sikre de bedste forudsætninger for opdagelse af og efterforskning af sikkerhedshændelser. Logningen skal ikke implementeres med formål om at monitorere brugeradfærd.* *Kravet er opfyldt, hvis der er implementeret logning på infrastrukturkomponenter i overensstemmelse med CFCS-vejledningen "Logning – en del af et godt cyberforsvar".* 30 dage er for kort en periode til at opbevare logs, fordi der ofte kan gå uger og måneder fra et angreb sker, til det bliver opdaget og undersøges nærmere via logs. Ud fra Rigsrevisionens tolkning (se fodnote 1) af dette minimumskrav og baggrunden i en vejledning fra Center for Cybersikkerhed kan Datatilsynet udlede, at der er tale om en type logning, som kræver mere end den, der er tale om i spørgsmål 4.3/4.4, fordi sidstnævnte fokuserer på at kunne udlede autoriserede personers anvendelser af personoplysninger, hvor 14.14 handler om at kunne opdage og stoppe hacking og dermed både autoriserede og uautoriserede personers eller softwares forsøg på at tilgå eller ødelægge data/it-systemer. Dermed er denne type logning også et værktøj, som evt. kan anvendes ifm. håndtering af brud på persondatasikkerheden, herunder underretning af berørte registrerede.	stk. 1 Databeskyttelsesforordningens artikel 33, stk. 3, litra c Databeskyttelsesforordningens artikel 34, stk. 2 ISO 27001:2013 – Anneks A.9.4.4 ISO 27001:2013 – Anneks A.12.4 1) Rigsrevisionens beretning af januar 2022 om "5 statslige myndigheders efterlevelse af 20 tekniske minimumskrav til it-sikkerheden"

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
Cyber- og informationssikkerhed	Domæner	14.15 Har organisationen sikret, at DNSSEC er tilknyttet alle domænenavne tilhørende organisationen?	Minimumskrav nr. 15 for statslige myndigheder er: *DNSSEC skal tilknyttes alle domænenavne tilhørende myndigheden.* *Formålet med kravet at sikre, at domæneforespørgsler besvares af domæneejeren, og at svar ikke er manipuleret undervejs. Ved brug af DNSSEC kan klienter kryptografisk stole på, at de tilgår de rette systemer og tjenester hos myndigheden.* *Kravet er opfyldt, hvis alle myndighedens domæner er DNSSEC-signerede.*	Databeskyttelsesforordningens artikel 32, stk. 1 ISO 27001:2013 – Anneks A.13.2.1
Cyber- og informationssikkerhed	Domæner	14.16 Anvender organisationen en Sikker DNS-tjeneste eller anden løsning, som beskytter organisationens brugere mod kendte skadelige websteder?	Minimumskrav nr. 16 for statslige myndigheder er: *Myndigheden skal anvende en Sikker DNS-tjeneste eller implementere anden løsning til beskyttelse mod adgang til kendte skadelige domæner.* *Formålet med kravet er at beskytte enheder på netværket mod at tilgå eksempelvis kendte phishingsider og hjemmesider med malware. Ved brug af en Sikker DNS-tjeneste filtreres navneforespørgsler på baggrund af automatisk opdaterede lister over domæner, der vurderes at være skadelige.* *Kravet er opfyldt, hvis 1) myndigheden anvender en Sikker DNS-tjeneste, eller der er implementeret en anden løsning, som yder tilsvarende beskyttelse mod skadelige domæner og 2) løsningen er baseret på vedligeholdte negativlister, der opdateres automatisk.*	Databeskyttelsesforordningens artikel 32, stk. 1 ISO 27001:2013 – Anneks A.12.2.1
Cyber- og informationssikkerhed	Domæner	14.17 Har organisationen implementeret DMARC REJECT-policy på alle domæner tilhørende organisationen?	Minimumskrav nr. 17 for statslige myndigheder er: *DMARC REJECT policy implementeres på alle domæner tilhørende myndigheden.*	Databeskyttelsesforordningens artikel 32,

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			Formålet med kravet er give mailmodtagere mulighed for at opdage forsøg på email-spoofing, hvor en afsender udgiver sig for at være en anden. Ved at implementere DMARC på alle domæner reduceres risikoen for myndighedens domænenavne kan misbruges til udsendelse af phishing- eller spam-mails. *Kravet er opfyldt, hvis: 1) DMARC er implementeret på alle myndighedens domæner og 2) DMARC politikken er sat til REJECT på alle myndighedens domæner og 3) SPF (Sender Policy Framework) og DKIM (DomainKeys Identified Mail) er implementeret på alle myndighedens domæner.*	stk. 1 ISO 27001:2013 – Anneks A.13.2.
Cyber- og informationssikkerhed	Netværk	14.18 Har organisationen sikret, at all Wi-Fi på organisationens arbejdsnetværk er krypteret med minimum WPA2?	Minimumskrav nr. 18 for statslige myndigheder er: *Myndighedens interne WiFi-netværk skal være krypteret med minimum WPA2.* *Formålet med kravet er at forhindre aflytning ved at foretage kryptering af trafikken på interne WiFi-netværk.* *Kravet er opfyldt, hvis trådløs adgang til myndighedens interne WiFi-netværk er krypteret med minimum WPA2.* *Kravet gælder ikke evt. gæstenetværk uden adgang til myndighedens systemer.* I tilgift til dette forventes det, at den kode, som anvendes til opkobling til WiFi, er tilstrækkelig lang og opbevares og videregives sikkert.	Databeskyttelsesforordningens artikel 25 Databeskyttelsesforordningens artikel 32, stk. 1 ISO 27001:2013 – Anneks A.13.2.1 ISO 27001:2013 – Anneks A.13.2.3 ISO

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
				27001:2013 – Anneks A.14.1
Cyber- og informationssikkerhed	Netværk	14.19 Har organisationen sikret, at alle eksterne webservere så vidt muligt er opdaterede, så snart producenten udgiver opdateringer?	Minimumskrav nr. 19 for statslige myndigheder er: *Software på myndighedens internetvendte tjenester skal holdes sikkerhedsopdateret.* *Formålet med kravet er at kendte sårbarheder bliver lukket hurtigst muligt. Derfor skal al software, der anvendes på myndighedens internetvendte tjenester, være omfattet af regelmæssig sikkerhedsopdatering.* *Kravet er opfyldt, hvis 1) det anvendte software og eventuelle tredjepartsbiblioteker på internetvendte systemer, er under aktiv support (dvs. der udgives sikkerhedsopdateringer fra producenten) og 2) der er indført tekniske og/eller organisatoriske foranstaltninger, der sikrer, at ikke-kritiske systemer sikkerhedsopdateres inden for 30 dage, og at kritiske systemer sikkerhedsopdateres hurtigst muligt inden da.* Idet formålet er at lukke eventuelle sårbarheder *hurtigst muligt* vil en "regelmæssig opdatering" fx én gang om året ikke opfylde formålet. At "sårbarheder lukkes hurtigst muligt" indebærer, at man skal reagere hurtigt ved opdagelsen af nye sårbarheder.	Databeskyttelsesforordningens artikel 32, stk. 1, litra b. ISO 27001:2013 – Anneks A.12.6.1
Cyber- og informationssikkerhed	Netværk	14.20 Krypterer organisationen al kommunikation til organisationens tjenester, hvor data transmitteres via internettet og andre netværk, som ikke er under den dataansvarliges kontrol, og denne kryptering er altid TLS 1.2 eller bedre?	Minimumskrav nr. 20 for statslige myndigheder er: *Adgang til myndighedens internetvendte tjenester, herunder hjemmesider, skal ske over en krypteret forbindelse.*	Databeskyttelsesforordningens artikel 32, stk. 1 ISO 27001:2013 –

Emne	Overskrift	Spørgsmål	Hjælpetekst	Reference
			Formålet med kravet er at sikre dataintegritet og fortrolighed samt forebyggelse af man-in-the-middle angreb. *Kravet er opfyldt, hvis alle myndighedens internetvendte tjenester kun kan anvendes over en krypteret forbindelse, herunder at: a) HTTP-tilgængelige tjenester automatisk omdirigerer til en HTTPS forbindelse og b) HTTPS-baserede tjenester kun understøtter TLS 1.2 eller højere og c) TLS krypterede forbindelser er baseret på konfigurationsparametrene i bilag 1 i* https://sikkerdigital.dk/Media/637962420328394595/Tekniske%20minimumskrav%20for%20statslige%20myndigheder%202023.pdf Rigsrevisionen lægger til grund (se fodnote 1), at selv om der kun er minimalt indhold på en webside, fx en placeholder, der viser, hvem der ejer websiden, så er hjemmesiden omfattet af kravet om kryptering. Bemærk at Datatilsynets spørgsmål også omfatter transmission over andre net end internettet, fx hvis der anvendes MPLS-netværk til udveksling af data mellem fysisk adskilte enheder i en organisation.	Anneks A.13.2.1 ISO 27001:2013 – Anneks A.13.2.2 1) Rigsrevisionens beretning af januar 2022 om "5 statslige myndigheders efterlevelse af 20 tekniske minimumskrav til it-sikkerheden"
15. Dokumentation				
Dokumentation		15.1 Kan organisationen inden for tre uger fremsende relevant dokumentation til Datatilsynet for de afgivne svar?	Datatilsynet vil efter omstændighederne kunne anmode om at få fremsendt dokumentation for en eller flere besvarelser.	Databeskyttelsesforordningen artikel 58, stk. 1, litra e