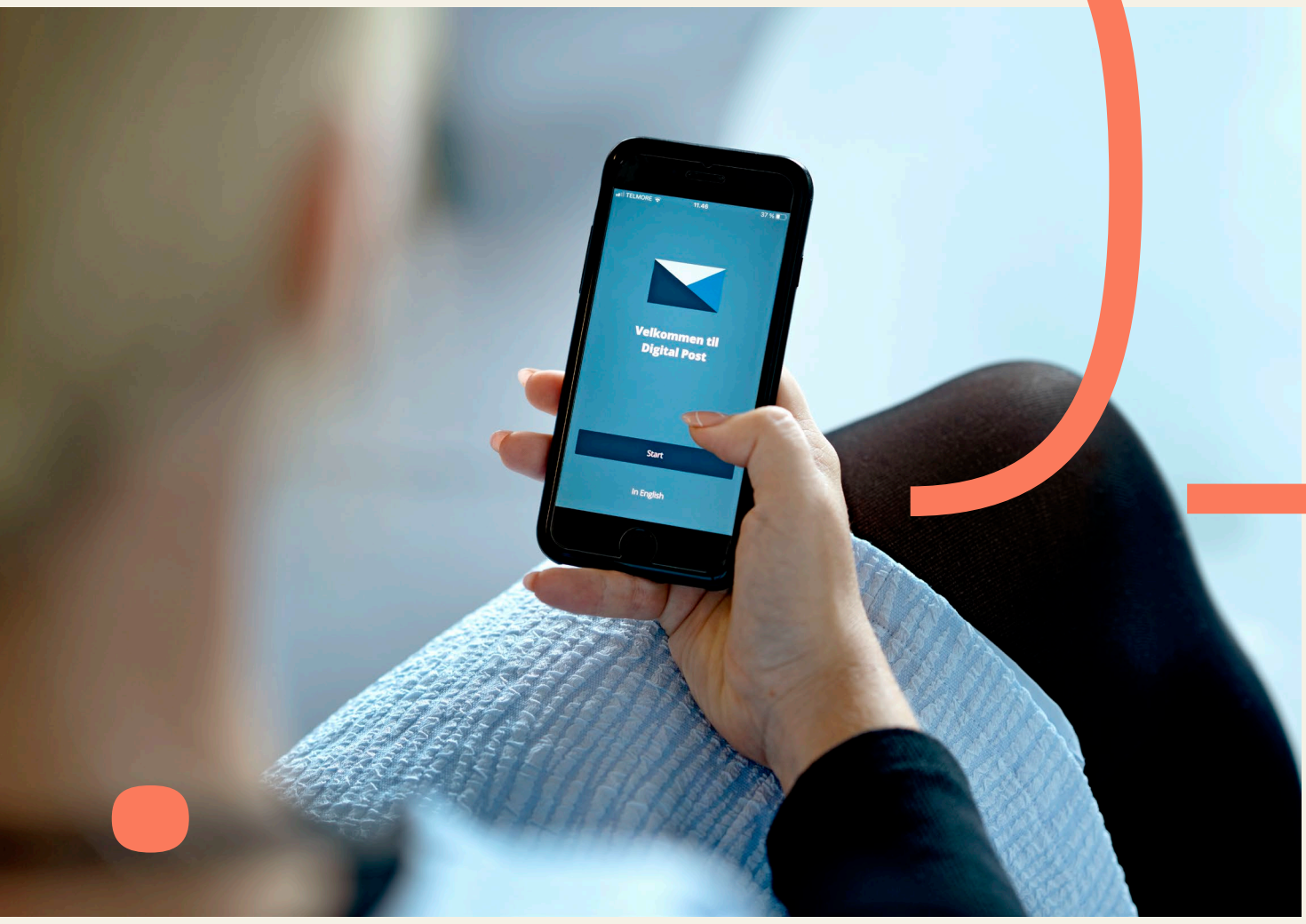
Digitaliserings-
styrelsen

Digital Post

Redegørelse om tilsyn med behandling af personoplysninger i 2024



Juli 2025

Indhold

Konklusion og oplysningspligt

Ledelsens sammenfattende konklusion samt oplysningspligt om Digitaliseringsstyrelsens tilsyn med behandling af personoplysninger i Digital Post.

Konklusion

Det vurderes, at Digitaliseringsstyrelsen som systemansvarlig for Digital Post har overholdt de databeskyttelsesretlige regler for behandling af personoplysninger, som beskrevet i bekendtgørelserne om behandling af personoplysninger i Digital Post[1].

Det overordnede billede viser, at Digitaliseringsstyrelsen har etableret en tilfredsstillende organisatorisk ledelse med informations- og persondatasikkerhed samt leverandørstyring med drift, udvikling og vedligehold af Digital Post. De undersøgte områder understøttes af fremlagt dokumentation for styring af forvaltningsopgaver med drift, udvikling og vedligehold af Digital Post.

Digitaliseringsstyrelsen har løbende forbedret arbejdsprocesserne omkring persondatasikkerheden med Digital Post, og der er leveret revisionsbevis for underleverandørens overholdelse af underdatabehandleraftalen.

For så vidt angår hændelseshåndtering i 2024 har Digitaliseringsstyrelsen registreret tre brud på persondatasikkerheden i Digital Post. De tre hændelser er meldt til Datatilsynet, som har afsluttet sagerne uden yderligere bemærkninger.

Om redegørelsen

Digitaliseringsstyrelsen har i 2025 gennemført tilsyn med behandling af personoplysninger i Digital Post for 2024 på vegne af de dataansvarlige offentlige afsendere og virksomheder.

Redegørelsen er udarbejdet jf. bekendtgørelserne med henblik på at stille de nødvendige oplysninger til rådighed for de dataansvarlige for at påvise overholdelse af de databeskyttelsesretlige regler.

I denne redegørelse beskrives det bagvedliggende tilsynsarbejde med Digital Post og resultatet af de gennemførte kontrolaktiviteter, som fremgår af kontrolkatalog sidst i redegørelsen.

Offentliggørelse af tilsynsmateriale

Til brug for de dataansvarliges eget tilsyn kan følgende tilsynsmateriale hentes på hjemmesiden digst.dk under menuen "It-løsninger" og "Digital Post":

- Digitaliseringsministeriets departements tilsynsrapport om Digitaliseringsstyrelsens tilsynspligt med behandling af personoplysninger i Digital Post for 2024
- Digitaliseringsstyrelsens redegørelse om tilsyn med behandling af personoplysninger i Digital Post i 2024

[1] Bekendtgørelse nr. 2019 af 29. oktober 2021 om ansvar, opgaver og tilsyn i forbindelse med behandlingen af personoplysninger i forbindelse med forsendelse af digital post fra offentlige afsendere.

Bekendtgørelse nr. 2020 af 29. oktober 2021 om ansvar, opgaver og tilsyn i forbindelse med behandlingen af personoplysninger indeholdt i meddelelser og opbevaringen heraf i juridiske enheders digitale postkasse.

- Notat om risici ved Digitaliseringsstyrelsens behandling af personoplysninger som databehandler
- Specifikke revisionserklæringer om Digital Post for perioden 2024 fra Digitaliseringsstyrelsens underleverandør.

Kontaktoplysninger

For at informere bredt til myndigheder, borgere og virksomheder og samtidigt skabe gennemsigtighed findes informationer om Digital Post-løsningen på Digitaliseringsstyrelsens hjemmeside digst.dk.

Ved henvendelser om de databeskyttelsesretlige regler på ministerområdet eller spørgsmål om tilsyn med persondatasikkerhed i Digital Post kan følgende kontaktes:

Digitaliseringsministeriets databeskyttelsesrådgiver

Generelle henvendelse om regler og rettigheder i forbindelse med behandlingen af personoplysninger inden for ministerområdet: dpo@digst.dk.

Digitaliseringsstyrelsens "Kontor for Digital Post"

Specifikke henvendelser vedrørende oplysningspligt om behandling af personoplysninger i Digital Post og redegørelsen: digitalpost@digst.dk.

Formål, retsgrundlag og dataansvar

Beskrivelse af formål, retsgrundlag, dataansvarskonstruktion og forhold omkring behandling af personoplysninger i Digital Post.

Regulering af Digitaliseringsstyrelsens databehandling for juridiske enheder og offentlige afsendere

Digital Post er er en sikker digital postkasse, som både borgere og virksomheder benytter til at modtage post fra offentlige myndigheder. Digitaliseringsstyrelsen er, i henhold til § 2 i lov om Digital Post (lovbekendtgørelse nr. 686 af 15. april 2021), udpeget til at sikre udvikling, drift, vedlige-holdelse og forvaltning af Digital Post-løsningen. I den forbindelse er Digitaliseringsstyrelsen dataansvarlig for behandlingen af personoplysninger, der sker for at indfri disse formål. Du kan læse mere om, hvordan Digitaliseringsstyrelsen behandler personoplysninger som dataansvarlig på Digitaliseringsstyrelsens hjemmeside: https://digst.dk/it-loesninger/digital-post/lovgivning/.

Efter § 2a, stk. 3-4 i lov om Digital Post er Digitaliseringsstyrelsen databehandler, når juridiske enheder og offentlige afsendere sender og modtager meddelelser via Digital Post. For juridiske enheder er Digitaliseringsstyrelsen også databehandler, hvis de juridiske enheder vælger at opbevare meddelelser i Digital Post.

Offentlige afsendere

Det er kun offentlige myndigheder, der kan blive offentlige afsendere. Det er Digitaliseringsstyrelsen, der administrerer, hvilke offentlige myndigheder, der kan blive tilsluttet Digital Post-løsningen. Når en offentlig myndighed er tilsluttet Digital Post, som offentlig afsender, kan den pågældende myndighed sende post til alle personer og virksomheder, som er tilsluttet Digital Post, jf. § 3, stk. 1-2 og § 4 i lov om Digital Post.

Offentlige afsendere har pligt til at oprette et system til modtagelse og opbevaring af postmeddelelser (herefter modtagersystem). Oprettelsen af et modtagersystem medfører, at Digitaliseringsstyrelsen ikke opbevarer meddelelser på vegne af offentlige afsendere, og som følge heraf er Digitaliseringsstyrelsen ikke databehandler for opbevaringen, jf. § 2 a, stk. 3 i lov om Digital Post.

Juridiske enheder

Omfatter alle juridiske enheder med CVR-nummer, der er registreret i Det Centrale Virksomhedsregister, herunder alle offentlige myndigheder, som ikke er tilsluttet Digital Post som offentlig afsender (se ovenfor). Juridiske enheder kan modtage og besvare meddelelser, der modtages via Digital Post. Digitaliseringsstyrelsen er databehandler både for forsendelsen og opbevaringen af meddelelser, som juridiske enheder, der ikke er offentlige afsendere, foretager via Digital Post, jf. § 2 a, stk. 4 i lov om Digital Post.

I henhold til artikel 28, stk. 3 i databeskyttelsesforordningen (GDPR), er der indgået to bekendtgørelser, der regulerer Digitaliseringsstyrelsens behandling af personoplysninger som databehandler på vegne af juridiske enheder og offentlige afsendere:

- Bekendtgørelse nr. 2019 af 29. oktober 2021 om ansvar, opgaver og tilsyn i forbindelse med behandlingen af personoplysninger i forbindelse med forsendelse af Digital Post fra offentlige afsendere.
- Bekendtgørelse nr. 2020 af 29. oktober 2021 om ansvar, opgaver og tilsyn i forbindelse med behandlingen af personoplysninger indeholdt i meddelelser og opbevaringen heraf i juridiske enheders digitale postkasse.

Begge bekendtgørelser fastlægger, at Digitaliseringsstyrelsen skal føre tilsyn med behandling af personoplysninger i Digital Post på vegne af de dataansvarlige og årligt udarbejde en redegørelse om tilsynsarbejdet, jf. § 13, stk. 2. Departementet i Digitaliseringsstyrelsen fører på baggrund heraf tilsyn med Digitaliseringsstyrelsen som databe-handler på vegne af de dataansvarlige juridiske enheder og offentlige afsendere.

I tillæg til redegørelsen er der foretaget en konsekvensanalyse af Digital Post-løsningen. I forbindelse med udførelsen af konsekvensanalysen, er der identificeret nogle risici, som kan være relevante for juridiske enheder og offentlige afsendere i forbindelse med tilsynet af Digital Post-løsningen. De identificerede risici er opsamlet i Bilag C. Risici ved Digitaliseringsstyrelsens behandling af personoplysninger som databehandler, som er offentliggjort på Digitaliseringsstyrelsens hjemmeside.

Information om revisionserklæringer

Digitaliseringsstyrelsen er ansvarlig for udvikling, drift, vedligeholdelse og forvaltning af Danmarks fællesoffentlige digitale postløsning, Digital Post.

Digitaliseringsstyrelsen har indgået it-kontrakter og tilslutningsaftaler med tredjepartsleverandører, der leverer it-ydelser til Digital Post og tjenester til visning af postmeddelelser i browser og mobil app. En tredjepartsleverandør (herefter underleverandør), er per definition ikke en del af Digitaliseringsstyrelsens organisation eller myndighed.

De daglige driftsopgaver med kernekomponenterne i driftsløsningen Digital Post er outsourcet til underleverandøren Netcompany. Til regulering af driftssamarbejdet og forpligtelser til overholdelse af regler om persondatabeskyttelse er der indgået it-kontrakt og underdatabehandleraftale mellem Netcompany og Digitaliseringsstyrelsen.

Som en del af Digitaliseringsstyrelsens systemforvaltning gennemføres et årligt leverandørtilsyn med efterlevelse af informations- og persondatasikkerheden baseret på revisionserklæringer afgivet af Netcompany. Revisionserklæringerne er udarbejdet af uafhængige statsautoriserede revisorer i henhold til indgået it-kontraktkrav om revision, sikkerhed og instruks i underdatabehandleraftale for Digital Post.

Ifølge bekendtgørelserne har Digitaliseringsstyrelsen, som databehandler, tilsynspligt med underleverandører, der behandler personoplysninger ved transmission og opbevaring af postmeddelelser i Digital Post. De dataansvarlige offentlige afsendere og virksomheder har ikke mulighed for at føre tilsyn direkte med underdatabehandlere uden Digitaliseringsstyrelsens forudgående skriftlige godkendelse, jf. § 8, stk. 6 i bekendtgørelserne.

Til brug for de dataansvarliges eget tilsyn stilles de to specifikke revisionserklæringer om Digital Post fra Netcompany til rådighed for de dataansvarlige på Digitaliseringsstyrelsens hjemmeside.

Revisionserklæringer for 2024 fra underleverandøren Netcompany

Netcompany har samlet set leveret fire revisionserklæringer for perioden 2024, som er fordelt på to generelle erklæringer, der er adresseret til alle Netcompanys kunder og to specifikke erklæringer til Digitaliseringsstyrelsen for Digital Post. Det skal bemærkes, at kun de to specifikke revisionserklæringer om Digital Post stilles til rådighed for de dataansvarlige.

De to generelle revisionserklæringer til kunderne dækker de generelle it-kontroller til driftsydelser og sikkerhedsforanstaltninger til databeskyttelse. Erklæringerne er udar-

bejdet for at opfylde almindelige behov for en bred kundekreds i Netcompanys driftsmiljø, herunder også dele af Digital Post driftsydelser.

De to specifikke revisionserklæringer om Digital Post er udarbejdet til Digitaliseringsstyrelsen. Erklæringerne omfatter udvalgte it-kontroller om sikkerhed til driftsydelser og sikkerhedsforanstaltninger til databeskyttelse af personoplysninger i Digital Post systemløsning hos Netcompany.

Tilsynet har noteret, at underleverandøren Netcompany har leveret revisionsmateriale i henhold til aftalte formalia i it-kontrakt, underdatabehandleraftale og udvalgte revisionskontroller. De årlige revisionserklæringer dækker perioden 1. januar 2024 til 31. december 2024 og er udfærdiget efter partielmetoden af det statsautoriserede revisionsselskab Deloitte.

Foruden enkelte mindre bemærkninger, som Netcompany har fulgt op på, og som revisor derfor ikke har yderligere bemærkninger til, har revisor ikke konstateret mangler eller afvigelser ved systemrevisionen, som har givet anledning til forbehold eller bemærkninger og dermed påvirket konklusionen af 2024 revisionserklæringerne. Revisors konklusion i de fire leverede erklæringer viser således, at implementering og kontroller i alle væsentlige henseender er tilfredsstillende samt effektive for at give høj grad af sikkerhed.

Foruden tilsyn med hovedleverandøren Netcompany gennemføres et tilsyn med underleverandører, som behandler personoplysninger i forbindelse med delopgaver til den digitale post-løsning. På Digitaliseringsstyrelsens hjemmeside fremgår listen over underleverandører.

Information om departementets it-tilsynsrapport

Digitaliseringsstyrelsen er underlagt et årligt overordnet ministerielt it-tilsyn af Digitaliseringsministeriets departement. Formålet med tilsynet er at give en overordnet vurdering af informationssikkerheden.

Tilsynet omfatter Digitaliseringsstyrelsens forpligtelser i forhold til ledelsesstyring af informationssikkerhed efter sikkerhedsstandarden ISO 27001, efterlevelse af databeskyttelsesforordningen og opfølgning på bemærkninger fra revisions- og tilsynsmyndigheder.

Departementet afgiver en årlig rapport for it-tilsyn med Digitaliseringsstyrelsens interne organisatoriske ledelsesstyring med informations- og persondatasikkerhed. Rapporten indeholder en vurdering af, om Digitaliseringsstyrelsens varetagelse af data foregår hensigtsmæssigt, pålideligt og sikkerhedsmæssigt forsvarligt, så fortrolighed, integritet og tilgængelighed sikres i nødvendigt omfang.

Departementets 2025 tilsynsrapport om Digitaliseringsstyrelsen

Digitaliseringsministeriets departement har i juni 2025 afgivet den årlige it-tilsynsrapport om det afsluttede tilsyn med informationssikkerhed i Digitaliseringsstyrelsen for 2024.

Af konklusionen fremgår det, at *"Digitaliseringsstyrelsen har, ud fra den foreviste dokumentation, etableret procedurer og kontroller, der sikrer en betryggende databeskyttelse og behandling af personoplysninger."*

Kontrolkatalog og kontrolmål

Til brug for gennemførelse af tilsynsaktiviteterne anvendes et kontrolkatalog. Kataloget består af en række fastlagte kontrolmål, der dækker krav ved behandling af personoplysninger ifølge §§ 4-12 i bekendtgørelserne om Digital Post. Kontrolmålene dækker de krav, som er beskrevet i bekendtgørelserne om Digital Post.

Kontrolkataloget indeholder kontrolmål og kontrolaktiviteter for følgende §§ relateret til Digitaliseringsstyrelsens databehandling af personoplysninger jf. bekendtgørelserne om Digital Post:

§ 4	Databehandleren handler efter instruks
§ 5	Fortrolighed
§ 6	Behandlingssikkerhed
§ 7	Autorisation og adgangskontrol
§ 8	Anvendelse af underdatabehandlere
§ 9	Overførsel til tredjelande eller internationale organisationer
§ 10	Bistand til den dataansvarlige
§ 11	Underretning om brud på persondatasikkerheden til Datatilsynet
§ 12	Sletning af personoplysninger

Kontrolkataloget danner grundlaget for Digitaliseringsstyrelsens dokumentation for efterlevelse af de pågældende krav og procedurer. Resultatet af det afsluttede tilsyn for perioden 2024 fremgår således i detaljer af kontrolkatalog herunder.

Kontrolkatalog for tilsyn med Digital Post udført i 2025

Nedenstående skema udgør dokumentation for resultatet af det afsluttede tilsyn i 2025 med persondatasikkerheden i Digital Post for perioden 2024.

§ 4 Databehandleren handler efter instruks				
Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolaktiviteter	Udført test	Yderligere bemærkninger
1.1	§4 Databehandleren handler efter instruks Stk 1-7 Digitaliseringsstyrelsen handler efter instruks fra den dataansvarlige offentlige afsender. Digitaliseringsstyrelsen instrueres som databehandler i at sende meddelelser for offentlige afsendere til de af de offentlige afsendere anførte modtageres digitale postkasser. Den dataansvarlige offentlige afsender kan give supplerende instruks, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk. Stk. 2. Databehandleren underretter omgående den dataansvarlige offentlige afsender, hvis en instruks efter vedkommendes mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret. Instruksen vil fortsat have virkning indtil lovligheden af instruksen afklares af Digitaliseringsstyrelsen, bistået af den dataansvarlige offentlige afsender. Den dataansvarlige offentlige afsender forbliver ansvarlig for databehandlerens fortsatte behandling af personoplysninger. Stk. 3. Denne bestemmelse udgør den databeskyttelsesretlige instruks i henhold til stk. 1. Nærmere oplysninger om selve behandlingen af personoplysninger fremgår af stk. 4 og henvisningerne i stk. 5. Omfanget af instruksen fremgår af henvisningerne i stk. 6. Stk. 4. Digitaliseringsstyrelsens behandling af personoplysninger består i transmission og levering af meddelelser med tilknyttede metadata sendt via Digital Post til de af de offentlige afsendere anførte modtagere, samt ved advisering af modtagerne via sms og e-mail ved levering af nye meddelelser og ved fremsendelse af servicebeskeder fra offent-	Ad stk. 1) og stk. 2): Kontor for Digital Post behandler personoplysninger efter instruks fra juridiske myndigheder. Ved modtagelse af supplerende instruks, foretager Kontor for Digital Post en vurdering af lovmedholdeligheden. Hvis Kontor for Digital Post vurderer, at der er noget til hinder for, at Kontor for Digital Post kan behandle personoplysninger for den juridiske enhed jf. den supplerende instruks, kontakter Kontor for Digital Post den juridiske enhed og fortsætter behandlingen af personoplysninger jf. Bekendtgørelse nr. 2019 af 29. oktober 2021 Ansvar, opgaver og tilsyn i forbindelse med behandlingen af personoplysninger i forbindelse med forsendelse af digital post fra offentlige afsendere. Bekendtgørelse nr. 2020 af 29. oktober 2021 Ansvar, opgaver og tilsyn i forbindelse med behandlingen af personoplysninger indeholdt i meddelelser og opbevaringen heraf i juridiske enheders digitale postkasse. Denne proces følger Kontor for Digital Posts interne procedurebeskrivelse om modtagelse, behandling og eventuelle implementering af supplerende instruks fra en juridisk enhed. Ad stk. 4): Dette er håndteret via det tekniske design i Digital Post. Ad stk. 5): Behandlingen af personoplysninger foregår som beskrevet i bekendtgørelsen	Stk. 1 og stk. 2) Der foreligger formaliserede procedurer, der sikrer, at Digitaliseringsstyrelsen identificerer, opbevarer og overholder en eventuel supplerende instruks fra de dataansvarlige offentlige afsendere og juridiske enhed. Der foreligger interne procedurer i Digitaliseringsstyrelsen og hos underleverandør om underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Digitaliseringsstyrelsens og underleverandørens procedurer indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i de dataansvarliges instruks eller ændringer i databehandlingen. De interne procedurer i Digitaliseringsstyrelsen og hos underleverandøren er opdaterede. Digitaliseringsstyrelsen kan fremvise en ajourført liste over de dataansvarlige, der har afgivet supplerende instruks samt de respektive instrukser. Ledelsen sikrer, at behandling af personoplysninger foregår i henhold til den eventuelle supplerende instruks fra de dataansvarlige. Behandlinger af personoplysninger foregår i overensstemmelse med den supplerende instruks fra de dataansvarlige. Stk. 4) Digital Post-løsningens arkitekturmål og tekniske design understøtter, at behandlingen af personoplysninger foregår som beskrevet i bekendtgørelsen. Stk. 5) Digitaliseringsstyrelsens databehandleraftale med leverandøren regulerer behandlingen af personoplysninger. Stk. 6) Der foreligger formaliserede procedurer, der sikrer, at Digitalise-	N/A

	lige afsendere via NemSMS. Digitaliseringsstyrelsens behandling af personoplysninger på vegne af de offentlige afsendere ophører således ved leveringen af meddelelserne til de af de offentlige afsendere anførte modtageres digitale postkasser samt ved leveringen af sms- og e-mail-advisering og ved fremsendelse af servicebeskeder fra offentlige afsendere via NemSMS. Stk. 5. Oplysninger om behandlingen af personoplysninger omfatter: 1) Formålet med behandlingen af personoplysninger, der fremgår af § 2, stk. 2. 2) Databehandlerens behandling af personoplysninger på vegne af de dataansvarlige offentlige afsendere drejer sig om transmission og levering af meddelelser sendt via Digital Post, der fremgår af stk. 4. 3) Behandlingen omfatter følgende typer af personoplysninger om de registrerede, der fremgår af § 3, stk. 1. 4) Behandlingen omfatter følgende kategorier af registrerede, der fremgår af § 3, stk. 2. 5) Databehandlerens behandling af personoplysninger på vegne af de dataansvarlige offentlige afsendere kan påbegyndes efter denne bekendtgørelses ikrafttræden. Behandlingen varer indtil bekendtgørelsen ophæves, jf. stk. 7. Stk. 6. Den offentlige afsender instruerer Digitaliseringsstyrelsen som databehandler vedrørende behandlingen af personoplysninger. Instruksen omfatter: 1) Behandlingens genstand/instruks, der fremgår af stk. 1 og 3. 2) Behandlingssikkerhed, der fremgår af § 6. 3) Bistand til den dataansvarlige, der fremgår af § 10. 4) Opbevaring og sletning, der fremgår af § 12. 5) Lokalitet for behandlingen, der fremgår af stk. 8.	og er reguleret i Digitaliseringsstyrelsens databehandleraftale med underleverandøren. Ad stk. 6): I forbindelse med Kontor for Digital Posts gennemgang og vurdering af en supplerende instruks fra en juridisk enhed, indgår en vurdering af, hvorvidt de i §4 stk. 6 nævnte punkter er beskrevet fyldestgørende. Dette fremgår af procedurebeskrivelsen og dokumentationen, som er angivet i kolonne E. Ad stk. 7): Kontor for Digital Post behandler personoplysninger i løsningen Digital Post så længe, at der er hjemmel til dette. Hvis bekendtgørelsen ophæves, stopper Kontor for Digital Post naturligvis med at behandle personoplysningerne i løsningen.	ringsstyrelsen gennemgår og vurderer, hvorvidt de nævnte punkter er beskrevet fyldestgørende i den supplerende instruks af den juridiske enhed, inden Digitaliseringsstyrelsen handler efter den supplerende instruks.	

	6) Instruks vedrørende overførsel af personoplysninger til tredjelande eller internationale organisationer, der fremgår af § 9. 7) Procedure for den dataansvarlige offentlige afsenders revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandlere, der fremgår af § 13. 8) Procedure for den dataansvarlige offentlige afsenders revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til underdatabehandlere, der fremgår af § 8, stk. 6. Stk. 7. Digitaliseringsstyrelsens behandling af personoplysninger i Digital Post på vegne af de dataansvarlige offentlige afsendere er ikke tidsbegrænset, men varer indtil bekendtgørelsen ophæves.			
Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolaktiviteter	Udført test	Yderligere bemærkninger
1.2	§ 4 Databehandleren handler efter instruks stk. 8 Stk. 8. Digital Post-løsningen er omfattet af lokationskravet i databeskyttelseslovens § 3, stk. 9, og bestemmelser udstedt i medfør heraf, hvorefter personoplysninger, der behandles i nærmere bestemte it-systemer, og som føres for den offentlige forvaltning, helt eller delvis alene må opbevares her i landet. Behandlingen og opbevaringen af personoplysninger skal ske i Danmark på baggrund af 1. pkt.	Ad stk. 8): Kontor for Digital Post har indgået en databehandleraftale med underleverandøren, som overholder denne del af bekendtgørelsen. Der foretages tilsyn med underleverandøren, og det fremgår af revisorerklæringerne.	Stk. 8) Digitaliseringsstyrelsen har opdaterede fortegnelser over behandlingsaktiviteter med angivelse af, at behandlinger foregår i Danmark. Der udføres review og vurdering af procedurer og retningslinjer for behandling samt opbevaring af data på lokationer i Danmark. Der fremgår godkendte underleverandører i databehandleraftalen mellem Digitaliseringsstyrelsen og underleverandør. Der foreligger underskrevne kontraktuelle aftaler mellem Digitaliseringsstyrelsen og underleverandør om lokationsgaranti. Der forefindes dokumentation for aftaler, procedurer og retningslinjer med underleverandør, at opbevaring af personoplysninger alene foretages på lokaliteter i Danmark.	N/A
	§ 5 Fortrolighed			
Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolaktiviteter	Udført test	Yderligere bemærkninger
2	§ 5 Fortrolighed stk. 1 Digitaliseringsstyrelsen skal som databehandler sikre, at de personer, der er autoriseret til at behandle per-	Ad stk. 1): Kontor for Digital Post er som resten af Digitaliseringsstyrelsen underlagt generelle retningslinjer om	Stk. 1) Der er indgået tavsheds- og fortrolighedsaftale med ansatte i Digitaliseringsstyrelsen, konsulenter og andre der bistår styrelsen.	N/A

	sonoplysninger på vegne af de offentlige afsendere har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.	tavshedserklæring og fortrolighedsaftaler for medarbejdere. Når Kontor for Digital Post indgår aftaler med konsulenter, sker dette ved brug af standardkontrakten, som anvendes i Digitaliseringsstyrelsen ved indkøb af konsulentbistand. Kontor for Digital Post har desuden indgået en databehandleraftale med underleverandøren, hvor der gælder de samme forhold i relation til tavshedserklæring og fortrolighedsaftaler for medarbejdere hos underleverandøren, som gælder for medarbejdere i Digitaliseringsstyrelsen og for konsulenter. Kontor for Digital Post har i øvrigt interne procedurer for, at Kontor for Digital Post mindst en gang årligt foretager review af proceduren for dokumentation af underleverandørens tavshedspligt. Gennem revisorerklæringerne sikrer Kontor for Digital Post, at underleverandøren lever op til sine forpligtelser.	Underleverandør er forpligtet til skriftlig tavsheds- og fortrolighedsaftale med medarbejdere. I revisionserklæringer fra underleverandør er det konstateret, at der foreligger dokumentation for tavsheds- og fortrolighedsaftale. Én gang årligt foretages der review af procedurer for dokumentation af underleverandørens tavshedspligt.	
		§ 6 Behandlingssikkerhed		
Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolaktiviteter	Udført test	Yderligere bemærkninger
3.1	§ 6. Behandlingssikkerhed Stk. 1-3 og stk. 5 Digitaliseringsstyrelsen iværksætter alle foranstaltninger, der kræves i henhold til databeskyttelsesforordningens artikel 32 og retshåndhævelseslovens § 27 om behandlingssikkerhed på baggrund af en risikovurdering. Digitaliseringsstyrelsen sikrer herved, at der under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der	Ad stk. 1): Kontor for Digital Post genbesøger årligt risikovurdering af løsningen samt tilhørende konsekvensanalyse. På baggrund af disse udfærdiges der et bilag C som stilles offentligt til rådighed for de dataansvarlige til brug for deres eget tilsyn. Ad stk. 2): På baggrund af den årlige risikovurdering og den tilhørende konsekvensanalyse foretager Kontor for Digital Post en vurdering af, om de fornødne tekniske og organisatoriske foranstaltninger er sat op, eller der er behov for yderligere.	Stk. 1) Der foreligger dokumentation for en ledelsesgodkendt risikovurdering af Digital Post, og der er implementeret foranstaltninger. Der er dokumentation for, at Digitaliseringsstyrelsen i rollen som databehandler har offentliggjort et selvstændigt notat om risici til de dataansvarlige, som tager afsæt i resultater fra risikovurderingen og konsekvensanalysen af Digital Post. Der er dokumentation for, at underleverandør har foretaget en risikovurdering og implementeret de tekniske foranstaltninger. Stk. 2) Der er dokumentation for, at Digitaliseringsstyrelsen har lavet årlig risikovurdering og i den tilhørende	N/A

	passer til disse risici. Digitaliseringsstyrelsen stiller på sin hjemmeside en sammenfatning af den foretagne risikovurdering til rådighed for de dataansvarlige offentlige afsendere, så risikovurderingen kan indgå i de dataansvarliges egne risikovurderinger. Stk. 2. Digitaliseringsstyrelsen gennemfører passende foranstaltninger for at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og tjenester ved at imødegå de i risikovurderingen identificerede risici. Der kan alt efter, hvad der er relevant, være tale om følgende foranstaltninger: 1) Kryptering af personoplysninger. 2) Logning af brug og adgang til personoplysninger. 3) Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af fysisk eller teknisk hændelse. 4) En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed. Stk. 3. Digitaliseringsstyrelsen fastsætter på baggrund af risikovurderingen, jf. § 6, stk. 1, og forslag til passende foranstaltninger, jf. § 6, stk. 2, nærmere interne bestemmelser om tekniske og organisatoriske sikkerhedsforanstaltninger, i eget informationssikkerhedsledelsessystem, for databehandlingen. 1) De interne bestemmelser gennemgås mindst én gang hvert år med henblik på at sikre, at de er fyldestgørende, og afspejler de faktiske forhold hos Digitaliseringsstyrelsen i rollen som databehandler. 2) Digitaliseringsstyrelsen giver den fornødne instruktion til egne medarbejdere, som behandler personoplysninger. Medarbejderne skal herunder gøres bekendt med de regler, der er fastsat i medfør af dette afsnit. Stk. 5. Digitaliseringsstyrelsen er ansvarlig for iagttagelse af reglen om databeskyttelse gennem design og databeskyttelse gennem standard-	Ad stk. 3): Det er intern sikkerhed, der har ansvaret for gennemgang af ISMS-politikken, og Kontor for Digital Post er underlagt disse interne bestemmelser. Digitaliseringsstyrelsens kontor for intern sikkerhed har ansvaret for at uddanne styrelsens medarbejdere i relevante databeskyttelsespolitikker og -procedurer. De skal desuden vurdere hvordan uddannelsen skal foregå, herunder ved relevante awarenessaktiviteter, interne oplæg, workshops etc. Derudover sørger Kontor for Digital Post som nævnt under §6 stk. 1 og stk. 2 naturligvis for at implementere eventuelle behov for ændringer, som bliver identificeret i forbindelse med den årlige risikovurdering og tilhørende konsekvensanalyse. I første omgang sker dette ved, at disse behov bliver tilføjet i den risikolog, som Kontor for Digital Post arbejder med i forhold til videreudviklingen af løsningen. Hvis der sker ændringer, får medarbejdere, der har adgang til personoplysninger, naturligvis besked om ændringernes karakter. Kontor for Digital Post følger desuden en proces for risikostyring. Herudover sikrer Kontor for Digital Post gennem kontrolmål i revisorerklæringer med underleverandøren, at underleverandørens medarbejdere modtager samme niveau af uddannelse og overholder samme krav i forhold til arbejdet med persondata. Ad stk. 5): For at sikre at Kontor for Digital Post fortsætter med at overholde reglen om databeskyttelse gennem design og databeskyttelse gennem	konsekvensanalyse foretager Digitaliseringsstyrelsen en vurdering af, om de fornødne tekniske og organisatoriske foranstaltninger er sat op, eller der er behov for yderligere. Der er dokumentation for, at underleverandør har foretaget en risikovurdering og implementeret de tekniske foranstaltninger. Stk. 3) Der er etableret et udvalg for informationssikkerhedsledelse og implementeret politikker, procedurer og retningslinjer i Digitaliseringsstyrelsen og hos underleverandør, som gennemgåes en gang om året. Digitaliseringsstyrelsen har givet de fornødne instruktioner til egne medarbejdere og underleverandør, som behandler personoplysninger. Digitaliseringsstyrelsen har stillet kontraktkrav til underleverandøren om årlig og regelmæssig awarenesstræning relateret til persondatasikkerhed, herunder at der foreligger revisionserklæringer fra underleverandøren om efterlevelse heraf. Digitaliseringsstyrelsen årligt og regelmæssigt uddanner og træner sine medarbejdere i persondatasikkerhed, herunder ved relevante awarenessaktiviteter, interne oplæg, workshops etc. Stk. 5) Der er procedurer for årlig afprøvning, vurdering og evaluering i Digitaliseringsstyrelsen og hos underleverandør.	

	indstillinger i databeskyttelsesforordningens artikel 25 og retshåndhævelseslovens § 20, stk. 2, jf. § 20, stk. 1, i forhold til udvikling, drift, vedligeholdelse og forvaltning af Digital Post.	standardindstillinger i databeskyttelsesforordningens artikel 25 og retshåndhævelseslovens § 20, stk. 2, jf. § 20, stk. 1, i forhold til udvikling, drift, vedligeholdelse og forvaltning af Digital Post laver Kontor for Digital Post en risikovurdering og en konsekvensanalyse, når der sker ændringer i løsningen.		
Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolaktiviteter	Udført test	Yderligere bemærkninger
3.2	§6 Behandlingssikkerhed Stk. 4 Den enkelte offentlige afsender er ansvarlig for at gennemføre egne relevante organisatoriske og tekniske sikkerhedsforanstaltninger, som knytter sig til den offentlige afsenders rolle som dataansvarlig i forbindelse med anvendelsen af Digital Post.	Ad stk. 4): Stk. 4 omhandler de offentlige afsendere og dermed ikke Kontor for Digital Post. Derfor har Kontor for Digital Post ikke kontrolaktiviteter ift. stk. 4.	N/A	N/A
	§ 7 Autorisation og adgangskontrol			
Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolaktiviteter	Udført test	Yderligere bemærkninger
4	§ 7 Autorisation og adgangskontrol Stk. 1-4 Kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles. De nærmere retningslinjer for denne autoriseringsordning er fastsat i dette afsnit. Stk. 2. Der må kun autoriseres personer, der beskæftiger sig med de formål, hvortil personoplysningerne behandles. De enkelte personer må ikke autoriseres til anvendelser, som de ikke har behov for. Stk. 3. Der må autoriseres personer, for hvem adgang til oplysninger er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver. Stk. 4. Kontrol af, hvorvidt de autoriserede personer fortsat skal have adgang til personoplysningerne, skal ske når det findes nødvendigt og mindst én gang hvert år.	Ad stk. 1): Kontor for Digital Post følger en intern proces for oprettelse og nedlæggelse af brugere. Ad stk. 2): Kontor for Digital Post autoriserer kun personer, der beskæftiger sig med formål, hvor der er behov for adgang til personoplysningerne i løsningen, og Kontor for Digital Post autoriserer kun disse personer i det omfang, der er nødvendigt for, at de kan udføre deres arbejde for Digitaliseringsstyrelsen. Kontor for Digital Post følger derfor også en intern procedure for styring af og kontrol med privilegerede rettigheder til løsningen. Ad stk. 3): Kontor for Digital Post autoriserer ikke andre personer end de medarbejdere hos Digitaliseringsstyrelsen, konsulenter og medarbejdere hos underleverandøren, som allerede er nævnt ovenfor under §5.	Stk. 1) Der er etableret proces for oprettelse og nedlæggelse af brugere i Digitaliseringsstyrelsen og hos underleverandør. Stk. 2) Der er procedurer for autorisation og løbende adgangskontrol i Digitaliseringsstyrelsen og hos underleverandør, som bliver ledelsesgodkendt. Der er proces for styring og kontrol med privilegerede rettigheder i Digitaliseringsstyrelsen og hos underleverandør, som ledelsesgodkendes. Stk. 3) Der er fastlagt faste perioder for kontroller med autorisation, adgang og rettigheder i Digitaliseringsstyrelsen og hos underleverandør. Stk. 4) Der er dokumentation for gennemførte kontroller med autorisation, adgang og rettigheder, herunder at dette sker mindst én gang årligt i Digitaliseringsstyrelsen og hos underleverandør.	N/A

		Ad stk 4): Kontor for Digital Post gennemfører kvartalsvist kontrol med, hvorvidt de autoriserede personer fortsat skal have adgang til personoplysninger.		
§ 8 Anvendelse af underdatabehandlere				
Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolaktiviteter	Udført test	Yderligere bemærkninger
5.1	§ 8 Anvendelse af underdatabehandlere Stk. 1-3 Stk. 1. Digitaliseringsstyrelsen har generel godkendelse til at anvende underdatabehandlere til Digital Post. Databehandleren vil underrette den dataansvarlige offentlige afsender på Digitaliseringsstyrelsens hjemmeside om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst en måneds varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Stk. 2. Ved anvendelse af underdatabehandlere er Digitaliseringsstyrelsen ansvarlig for at efterleve kravene i databeskyttelsesforordningens artikel 28 og retshåndhævelseslovens § 22. Digitaliseringsstyrelsen er herefter blandt andet forpligtet til: 1) Alene at anvende underdatadatabehandlere, der kan stille de fornødne garantier for, at de gennemfører de passende tekniske og organisatoriske sikkerhedsforanstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder. 2) At sikre at der foreligger en gyldig underdatabehandleraftale mellem Digitaliseringsstyrelsen og en eventuel underdatabehandler. Stk. 3. Digitaliseringsstyrelsens underdatabehandlere for Digital Post vil fremgå af Digitaliseringsstyrelsens hjemmeside. Oplysninger om underdatabehandlere kan fremsendes til de offentlige afsendere efter skriftlig anmodning herom til Digitaliseringsstyrelsen.	Ad stk. 1): Kontor for Digital Post er databehandler, mens underleverandørerne er underdatabehandlere. Digitaliseringsstyrelsen har angivet underdatabehandlere for Digital Post på Digitaliseringsstyrelsens hjemmeside. Digitaliseringsstyrelsen opdaterer listen over underdatabehandlere, hvis der sker ændringer. Ad stk. 2, 1): Kontor for Digital Post har i kontrakten og databehandleraftalen med underleverandøren af Digital Post stillet krav til, at underleverandøren kan stille de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger. Kontor for Digital Post sikrer, at denne del af aftalen overholdes gennem kontrolmål i revisorerklæringer, der modtages årligt. Følgende underleverandører nævnes også på listen over underdatabehandlere for Digital Post: Fellowmind: behandler ikke personooplysninger. SIT: Finansministeriet fører tilsyn. Erhvervsstyrelsen: KØS fører tilsyn. Ad stk. 2, 2): Kontor for Digital Post følger JURs vejledninger og skabeloner til brug for indgåelse af gyldige databehandleraftaler. Databehandleraftalen med Leverandøren er bygget op efter denne skabelon, og aftalen gennemgås mindst en gang årligt med henblik på evt. opdatering.	Stk. 1) Overblikket er opdateret og offentliggjort på Digitaliseringsstyrelsens hjemmeside. Stk. 2) Der er indgået kontrakt og databehandleraftale, som sikrer de fornødne garantier for, at underleverandøren gennemfører passende tekniske og organisatoriske sikkerhedsforanstaltninger. Der er indgået en gyldig underskrevet underdatabehandleraftale mellem Digitaliseringsstyrelsen og underleverandør. Stk. 3) Digitaliseringsstyrelsen har offentliggjort informationer om underdatabehandlere på hjemmeside.	N/A

		Ad stk. 3): Se §8 stk. 1.		
Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolaktiviteter	Udført test	Yderligere bemærkninger
5.2	§ 8 Anvendelse af underdatabehandlere stk. 4-5 Stk. 4. Digitaliseringsstyrelsen sørger for at pålægge underdatabehandlere de samme databeskyttelsesforpligtelser, som dem, der er fastsat ved denne bekendtgørelse, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i henholdsvis databeskyttelsesforordningen eller retshåndhævelsesloven. Stk. 5. Digitaliseringsstyrelsen er således ansvarlig for – igennem indgåelsen af en underdatabehandleraftale – at pålægge en eventuel underdatabehandler mindst de forpligtelser, som Digitaliseringsstyrelsen selv er underlagt efter databeskyttelsesreglerne og denne bekendtgørelse.	Ad stk. 4-5): Kontor for Digital Post er databehandler, mens underleverandørerne er underdatabehandlere. Kontor for Digital Post har i kontrakten og databehandleraftalen med underleverandøren til Digital Post sikret, at underleverandøren skal leve op til samme databeskyttelsesforpligtigelser, som fremgår af denne bekendtgørelse. Kontor for Digital Post har en årlig gennemgang af databehandleraftalen med henblik på, om kontrakten overholder dansk lovgivning, EU-lovgivning, databeskyttelsesregler og bekendtgørelser.	Stk. 4) Der er indgået en juridisk bindende kontrakt og aftale mellem Digitaliseringsstyrelsen og underleverandøren, som til enhver tid forpligter leverandøren til at overholde EU og dansk lovgivning, databeskyttelsesregler og bekendtgørelser. Stk. 5) Digitaliseringsstyrelsen har etableret processer som sikrer, at kontrakter og aftaler med tredjepartsleverandører er juridisk bindende, og leverandørerne pålægges at overholde europæisk og dansk lovgivning. Digitaliseringsstyrelsen har stillet krav og vilkår til underleverandøren om indgåelse af underdatabehandleraftale ved behandling af personoplysninger hos underleverandørens leverandør.	N/A
Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolaktiviteter	Udført test	Yderligere bemærkninger
5.3	§8 Anvendelse af underdatabehandlere stk. 6-7 Stk. 6. Digitaliseringsstyrelsen fører tilsyn med underdatabehandlerens overholdelse af underdatabehandleraftalen. De dataansvarlige har ikke mulighed for at føre tilsyn direkte med underdatabehandleren uden Digitaliseringsstyrelsens forudgående skriftlige godkendelse. De dataansvarlige får, til brug for eget tilsyn, mulighed for at modtage relevante informationer, som Digitaliseringsstyrelsen gennem tilsynet med underdatabehandleren, stiller til rådighed, jf. § 13, stk. 2. Tilsynet med underdatabehandlere udføres blandt andet ved at: 1) Underdatabehandleren én gang årligt skal indhente en revisorerklæring i overensstemmelse med aktuelle standarder for GDPR-revisorerklæringer fra en uafhængig revisor	Ad stk. 6): Kontor for Digital Post har månedlige driftmøder med underleverandøren til Digital Post-løsningen og føre årlige tilsyn med samme. Ad stk. 6, 1): Det årlige tilsyn inkluderer, at underleverandøren fremlægger en revisorerklæring for deres behandling af persondata. Ad stk. 6, 2): I ovennævnte revisorerklæringer omhandler kontrolmål B.15 den fysiske sikkerhed: "Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger."	Stk. 6) Digitaliseringsstyrelsen har etableret model og proces for årlig underleverandørtilsyn med overholdelse af underdatabehandleraftaler. Der foreligger ledelsesgodkendt dokumentation for gennemført underleverandørtilsyn med overholdelse af underdatabehandleraftaler. 1) Digitaliseringsstyrelsen har indhentet en revisorerklæring i overensstemmelse med aktuelle standarder for GDPR-revisorerklæringer fra en uafhængig revisor angående underdatabehandleren og dennes eventuelle underdatabehandleres behandling af informationssikkerhed og personoplysninger Digitaliseringsstyrelsen har stillet de årlige revisionserklæringer fra underleverandør til rådighed for de dataansvarlige.	N/A

	angående underdatabehandleren og dennes eventuelle underdatabehandleres behandling af informationssikkerhed og personoplysninger i medfør af den til enhver tid gældende underdatabehandleraftale. Digitaliseringsstyrelsen modtager revisorerklæringen fra underdatabehandleren, hvorefter den stilles til rådighed for de dataansvarlige offentlige afsendere. 2) Digitaliseringsstyrelsen, eller en uafhængig revisor bemyndiget af Digitaliseringsstyrelsen, har ret til at foretage inspektioner af underdatabehandlerens fysiske faciliteter, hvor der behandles personoplysninger samt modtage de nødvendige informationer til udførelsen af undersøgelsen af, hvorvidt underdatabehandleren har truffet de sikkerhedsforanstaltninger, der følger af underdatabehandleraftalen samt gældende databeskyttelsesret. 3) Digitaliseringsstyrelsen har løbende mulighed for at indhente informationer baseret på resultaterne af enten revisorerklæringen, inspektionen af de fysiske faciliteter eller de modtagende informationer. Når der er behov for det, er Digitaliseringsstyrelsen berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og denne bekendtgørelse. 4) Underdatabehandleren skal give myndigheder, eller deres udpegede repræsentanter, der efter EU-retten eller lovgivningen i en medlemsstat har ret til adgang til Digitaliseringsstyrelsens og underdatabehandlerens faciliteter, adgang til underdatabehandlerens fysiske faciliteter mod forevisning af behørig legitimation. Stk. 7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver Digitaliseringsstyrelsen fuldt ansvarlig over for de dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.	Ad stk. 6, 3): Der er i Kontor for Digital Post en intern arbejdsgang, som sikrer, at der startes en dialog med underdatabehandleren om udbedring, hvis der ved gennemgang af ovennævnte revisorerklæring, er udeståender. Ad stk. 6, 4): Ved ønske og behørig legitimation fra den dataansvarlige, vil Kontor for Digital Post sikre den dataansvarliges mulighed for adgang til de fysiske faciliteter. Ad stk. 7): Kontor for Digital Post er opmærksomme på, at Digitaliseringsstyrelsen har ansvaret for, at underdatabehandlere opfylder deres databeskyttelsesforpligtelser, og sikrer gennem den løbende leverandørstyring, vores processer for incident og problem management sammen med leverandøren samt revisorerklæring fra Leverandøren, at Leverandøren, som i denne henseende er underdatabehandlere, lever op til samme krav som Digitaliseringsstyrelsen krav til Leverandøren jf. § 8, stk. 4. Formålet med proceduren for håndtering af incidents er at sikre, at opståede og indrapporterede incident håndteres korrekt jf. leverandøraftaler, samt processer for sikkerhedshændelser.	2) Digitaliseringsstyrelsen har stillet krav i kontrakt og databehandleraftale med underleverandøren for Digital Post, og kan dermed foretage inspektioner af underdatabehandlerens fysiske faciliteter og modtage de nødvendige informationer til udførelsen af undersøgelsen af, hvorvidt underdatabehandleren har truffet de nødvendige sikkerhedsforanstaltninger. Der er ingen bemærkninger i revisionserklæringer omkring fysisk sikkerhed hos underleverandøren. 3) Der er skrevet databehandleraftale og kontraktkrav med underleverandør om, at Digitaliseringsstyrelsen har løbende mulighed for at indhente informationer baseret på resultaterne af enten revisorerklæringen, inspektionen af de fysiske faciliteter eller de modtagende informationer. Når der er behov for det, er Digitaliseringsstyrelsen berettiget til at anmode om gennemførelse af yderligere foranstaltninger for at overholde nævnte krav og bekendtgørelser 4) Der har ikke været ønske om adgang til de fysiske faciliteter. Stk. 7) Der er procedurer for håndtering af incidents, og at der er kontraktkrav om incidentshåndtering hos underleverandør.	

§ 9 Overførsel til tredjelande eller internationale organisationer				
Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolaktiviteter	Udført test	Yderligere bemærkninger
6	§ 9 Overførsel til tredjelande eller internationale organisationer Stk. 1-4 Digitaliseringsstyrelsen vil som databehandler for Digital Post ikke overføre personoplysninger til tredjelande eller internationale organisationer, jf. § 4, stk. 8. Stk. 2. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må derfor kun foretages af Digitaliseringsstyrelsen på baggrund af dokumenteret instruks herom fra den dataansvarlige offentlige afsender og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V og retshåndhævelseslovens afsnit VII. Uden dokumenteret instruks fra den dataansvarlige offentlige afsender kan Digitaliseringsstyrelsen således ikke inden for rammerne af denne bekendtgørelse: 1) Overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation. 2) Overlade behandling af personoplysninger til en underdatabehandler i et tredjeland. 3) Behandle personoplysningerne i et tredjeland. Stk. 3. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som Digitaliseringsstyrelsen ikke er blevet instrueret i at foretage af den dataansvarlige offentlige afsender, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Digitaliseringsstyrelsen er underlagt, skal Digitaliseringsstyrelsen underrette den dataansvarlige offentlige afsender om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser. Stk. 4. Ved overførsler omfattet af stk. 2, er den offentlige afsender ansvarlig for at sikre, at der foreligger et gyldigt overførselsgrundlag i hen-	Ad stk. 1): Kontor for Digital Post har gennem databehandleraftalen med underleverandøren sikret, at der ikke sker overførelse af personoplysninger til tredjelande eller internationale organisationer. Dette kontrolleres gennem revisorerklæringerne modtaget fra underleverandøren. Ad stk 2): Kontor for Digital Post handler udelukkende på baggrund af instruks fra den dataansvarlige og vil behandle en instruks fra en dataansvarlig om overførsel af personoplysninger til tredjelande eller internationale organisationer som en supplerende instruks (se §4, stk. 1-2). Ad. Stk. 2, 1-3): Kontor for Digital Post vil derfor ikke uden dokumenteret instruks: 1) overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation 2) overlade persondatabehandlingen til en underdatabehandler i tredjeland 3) behandle personoplysninger i et tredjeland Ad stk. 3): Kontor for Digital Post overholder bekendtgørelsen og vil underrette den dataansvarlige offentlige afsender, hvis overførsel af personoplysninger til tredjelande eller internationale organisationer kræves i henhold til EU-ret eller medlemsstaternes nationale ret. Kontor for Digital Post har endnu ikke prøvet at modtage en sådan henvendelse, men forventer, at det vil ske via Digital Posts postkasse. Ad stk. 4): I de tilfælde hvor den dataansvarlige har ud-	Stk. 1-4) Der er en databehandleraftale med underleverandør, om at der ikke må overføres personoplysninger til tredjelande eller internationale organisationer. Dertil er revisionserklæring fra underleverandør ISAE3000 revisionserklæring inspiceret. Stk. 2) Verificeret, at der er dokumentation for, at Digitaliseringsstyrelsens overførsler sker efter aftale, godkendelse og instruks fra den dataansvarlige. Stk. 3) Digitaliseringsstyrelsen vil følge proceduren som beskrevet i bekendtgørelsen. Stk. 4) Digitaliseringsstyrelsens overførsler sker efter aftale, godkendelse og instruks fra den dataansvarlige.	N/A

	hold til databeskyttelsesforordningens kapitel V og retshåndhævelseslovens afsnit VII, kapitel 17.	stedt en instruks om overførelse til et tredjeland eller en international organisation, er det samme dataansvarliges ansvar at sikre, at der foreligger et gyldigt overførelsesgrundlag. Kontor for Digital Post udfører kontrolaktiviteter som beskrevet under §4 stk. 1-2 ved modtagelse af en dokumenteret instruks, som beskrevet i §9, men foretager ikke yderligere kontrolaktiviteter ift. §9 stk. 4.		
§ 10 Bistand til den dataansvarlige				
Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolaktiviteter	Udført test	Yderligere bemærkninger
7.1	§ 10 BISTAND TIL DEN DATAANSVARLIGE Stk. 1-2 Digitaliseringsstyrelsen bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den offentlige afsenders forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder, som er fastlagt i databeskyttelsesforordningens kapitel III og retshåndhævelseslovens kapitel 5-6. Stk. 2. Digitaliseringsstyrelsen skal i medfør af stk. 1, så vidt muligt skal bistå den offentlige afsender i forbindelse med, at den offentlige afsender i dens rolle som dataansvarlig skal sikre overholdelsen af nedenstående regler i databeskyttelsesforordningen og retshåndhævelsesloven: 1) Oplysningspligten ved indsamling af personoplysninger hos den registrerede, jf. databeskyttelsesforordningens artikel 13. 2) Oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede, jf. databeskyttelsesforordningens artikel 14. 3) Den registreredes indsigtsret, jf. databeskyttelsesforordningens artikel 15 og retshåndhævelseslovens § 15. 4) Retten til berigtigelse, jf. databeskyttelsesforordningens artikel 16 og	Ad. stk. 1 og stk. 2, 1-8): Kontor for Digital Post følger en intern procedure med årligt genbesøg og opdatering af privatlivspolitikken, hvilket fremgår af Kontor for Digital Posts årshjul. Kontor for Digital Post publicerer privatlivspolitikken for borgere på Digitaliseringsstyrelsens hjemmeside.	Stk. 1-2) Digitaliseringsstyrelsen har procedurer vedrørende bistand til de dataansvarlige, herunder offentliggørelse af informationer på hjemmeside om Digital Post og hvordan bistand skal finde sted til de registrerede i forbindelse med: udlevering, rettelser, sletning, begrænsning af oplysninger, underretningspligt og retten til indsigelser. Der findes diagram med dataflow og dokumentation for, at it-systemer hos underleverandør understøtter procedurer for bistand til de registrerede. Der foretages løbende - og mindst én gang årligt - vurdering af, om procedurerne skal opdateres.	N/A

	retshåndhævelseslovens § 17, stk. 1. 5) Retten til sletning (»retten til at blive glemt«), jf. databeskyttelsesforordningens artikel 17 og retshåndhævelseslovens § 17, stk. 2. 6) Retten til begrænsning af behandling, jf. databeskyttelsesforordningens artikel 18 og retshåndhævelseslovens § 17, stk. 3. 7) Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling, jf. databeskyttelsesforordningens artikel 19. 8) Retten til indsigelse, jf. databeskyttelsesforordningens artikel 21.			
Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolaktiviteter	Udført test	Yderligere bemærkninger
7.2	§ 10 BISTAND TIL DEN DATAANSVARLIGE Stk. 3 Stk. 3. Digitaliseringsstyrelsen bistår den dataansvarlige med at sikre overholdelse af den offentlige afsenders forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 og retshåndhævelseslovens §§ 25-29 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Digitaliseringsstyrelsen som databehandler, jf. databeskyttelsesforordningens artikel 28, stk. 3, litra f og retshåndhævelseslovens § 27, stk. 1. Dette indebærer, at Digitaliseringsstyrelsen under hensyntagen til behandlingens karakter skal bistå den enkelte offentlige afsender i forbindelse med, at denne skal sikre overholdelsen af: 1) Forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen, jf. § 6. 2) Forpligtelsen til at anmelde brud på persondatasikkerheden til Datatilsynet uden unødig forsinkelse og om muligt senest 72 timer, efter at den enkelte dataansvarlige er blevet bekendt med bruddet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, jf. § 11.	Ad stk. 3): Kontor for Digital Post bistår den dataansvarlige i deres overholdelse af den offentlige afsenders forpligtigelser i medfør af databeskyttelsesforordningens artikel 32-36 og retshåndhævelseslovens §§25-29 ved, at: Ad 1): Kontor for Digital Post genbesøger årligt risikovurdering af løsningen samt tilhørende konsekvensanalyse. På baggrund af den årlige risikovurdering og den tilhørende konsekvensanalyse foretager Kontor for Digital Post en vurdering af, om de fornødne tekniske og organisatoriske foranstaltninger er sat op, eller der er behov for yderligere. På baggrund af risikovurderingen og konsekvensanalysen udfærdiges bilag C, som på Digitaliseringsstyrelsens hjemmeside stilles offentligt til rådighed for de dataansvarlige til brug for deres eget tilsyn. Ad 2): Kontor for Digital Post følger en intern procedure for anmeldelse af persondatabrud senest 72 timer efter bruddet til den dataansvarlige.	1) Digitaliseringsstyrelsen opdaterer løbende og mindst en gang årligt risikobilledet og foranstaltninger på baggrund af en fornyet risiko- og trusselsvurdering. Bilag c er offentliggjort på DIGST.dk. 2) Der er en procedure for anmeldelse af databrud inden for 72 timer, og at der foretages løbende og mindst én gang årligt en vurdering af, om procedurerne skal opdateres. 3) Digitaliseringsstyrelsen har etableret procedurer og retningslinjer for behandling af brud på persondatasikkerheden, som sikrer, at de dataansvarlige bliver underrettet rettidigt, når et brud sandsynligvis vil indebære en høj risiko for de registreredes rettigheder. Der foreligger kontraktkrav og underdatabehandleraftale med underleverandøren som, sikrer, at der er etableret procedurer for bistand til Digitaliseringsstyrelsen ved underretning til de dataansvarlige og anmeldelse til Datatilsynet, herunder evt. underretningsbrev om karakteren af bruddet, konsekvenser og mulige foranstaltninger til håndtering af bruddet. Digitaliseringsstyrelsen opdaterer løbende og mindst en gang årligt procedurer og retningslinjer vedrørende håndtering af underretning om brud på persondatasikkerheden.	N/A

	3) Forpligtelsen til uden unødig forsinkelse at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, jf. § 11. 4) Forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, og forpligtelsen til at høre Datatilsynet inden behandling, hvis en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den enkelte dataansvarlige for at begrænse risikoen.	Kontor for Digital Post sikrer ved en årlig gennemgang, at proceduren er opdateret. Ad 3): Kontor for Digital Post følger en intern procedure for underretning af den/de registrerede om persondatabrud. Der er ligeledes i Kontor for Digital Post en skabelon for underretningsbrev. Både skabelon og procedure gennemgås en gang årligt med henblik på evt. opdatering. Ad 4): Kontor for Digital Post genbesøger årligt risikovurdering af løsningen samt tilhørende konsekvensanalyse. På baggrund af risikovurderingen og konsekvensanalysen udfærdiges bilag C, som på Digitaliseringsstyrelsens hjemmeside stilles offentligt til rådighed for de dataansvarlige til brug for deres eget tilsyn.	4) Digitaliseringsstyrelsen har etableret procedurer, som sikrer rettidig bistand til den dataansvarlige med at overholde forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse. Digitaliseringsstyrelsen vurderer løbende og mindst en gang årligt om procedurer skal opdateres. Digitaliseringsstyrelsen har offentliggjort selvstændigt notat om risici, som bistand til de dataansvarliges arbejde med egen konsekvensanalyse samt valg af foranstaltninger til begrænsning af risici, såfremt det vurderes nødvendigt.	

§ 11 Underretning om brud på persondatasikkerheden til Datatilsynet

Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolaktiviteter	Udført test	Yderligere bemærkninger
8	§ 11 Underretning om brud på persondatasikkerhed til Datatilsynet Stk. 1-4 Digitaliseringsstyrelsen underretter uden unødig forsinkelse den dataansvarlige offentlige afsender efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden. Stk. 2. Digitaliseringsstyrelsens underretning til den dataansvarlige offentlige afsender skal ske uden unødig forsinkelse og senest 48 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige offentlige afsender kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til Datatilsynet, jf. databeskyttelsesforordningens artikel 33 og retshåndhævelseslovens § 28. Den offentlige afsender underretter de registrerede om bruddet på persondatasikkerheden i overensstemmelse med kravene herom i databeskyttelsesforordningens artikel 34 og retshåndhævelseslovens § 29.	Ad stk. 1): Kontor for Digital Post følger en intern proces, der sikrer underretning af dataansvarlige uden unødig forsinkelse. Kontor for digital Post sikrer desuden gennem databehandleraftalen med underleverandøren, at underleverandøren bistår ved databrud. Ad stk. 2): Kontor for Digital Post følger en intern procedure, der sikrer, at den dataansvarlige informeres inden for 48 timer fra det tidspunkt, hvor Kontor for Digital Post har fået kendskab til, at der er sket et databrud. Kontor for Digital Post sikrer desuden gennem databehandleraftalen med underleverandøren, at underleverandøren bistår ved databrud.	Stk. 1) Digitaliseringsstyrelsen har etableret procedurer og retningslinjer for behandling af brud på persondatasikkerheden, som sikrer, at de dataansvarlige bliver underrettet rettidigt indenfor 48 timer, når der er konstateret sandsynlighed for brud på persondatasikkerheden. Med årshjulet for Digital post sikres, at procedurer og databehandleraftaler med Netcompany vurderes og opdateres en gang årligt. Stk. 2) Der foreligger kontraktkrav og underdatabehandleraftale med underleverandøren, som sikrer, at der er etableret procedurer for bistand til Digitaliseringsstyrelsen ved underretning til de dataansvarlige indenfor 48 timer og anmeldelse til Datatilsynet senest 72 timer, herunder evt. underretningsbrev om karakteren af bruddet, konsekvenser og mulige foranstaltninger til håndtering af bruddet.	N/A

	Stk. 3. Digitaliseringsstyrelsen kan på vegne af samtlige dataansvarlige offentlige afsendere omfattet af denne bekendtgørelse, under hensyn til sagens karakter, bruddets omfang og såfremt bruddet omfatter Digital Post-løsningen, foretage en samlet anmeldelse til Datatilsynet i overensstemmelse med databeskyttelsesforordningens artikel 33, stk. 1 og retshåndhævelseslovens § 28, stk. 1 og stk. 2. Digitaliseringsstyrelsen underretter uden unødig forsinkelse den dataansvarlige offentlige afsender efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden, og inden en samlet anmeldelse sendes til Datatilsynet. Stk. 4. I overensstemmelse med stk. 1 skal Digitaliseringsstyrelsen bistå den offentlige afsender med at foretage anmeldelse af bruddet til Datatilsynet. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som i medfør af databeskyttelsesforordningens artikel 33, stk. 3 og retshåndhævelseslovens § 28, stk. 3, skal fremgå af den dataansvarlige offentlige afsenders anmeldelse af bruddet til Datatilsynet: 1) Karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger. 2) De sandsynlige konsekvenser af bruddet på persondatasikkerheden. 3) De foranstaltninger, som Digitaliseringsstyrelsen har udført som databehandler, og de foranstaltninger som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.	Ad stk. 3): Digitaliseringsstyrelsen har mulighed for at lave en anmeldelse til Datatilsynet på vegne af de dataansvarlige, hvilket vil ske efter aftale med de dataansvarlige. Derfor vil dette blive behandlet som en supplerende instruks. Ad stk. 4): Som nævnt i stk. 1 følger Kontor for Digital Post en intern procedure for at bistå den dataansvarlige i at foretage anmeldelse til datatilsynet ved persondatabrud.	Stk. 3) Der er porcedurer for modtagelse af supplerende instruks fra offentlige afsendere og juridiske enheder. Stk. 4) Der er etableret procedurer og retningslinjer for behandling af brud på persondatasikkerheden, som sikrer, at Digitaliseringsstyrelsen kan bistå den dataansvarlige i at foretage anmeldelse til datatilsynet ved persondatabrud.	

§ 12 Sletning af personoplysninger (For offentlige afsendere og juridiske enheder)				
Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolaktiviteter	Udført test	Yderligere bemærkninger
9.1	§12 Sletning af personoplysninger for offentlige afsendere (BEK nr 2019 af 29/10/2021)	Ad stk. 1): Dette er håndteret via det tekniske design i	Stk. 1) Databehandleraftale med underleverandør og arkitekturmål understøtter, at databehandling sker som beskrevet i §12.	N/A

	Digitaliseringsstyrelsens databehandling i medfør af denne bekendtgørelse ophører med levering af meddelelserne og ved leveringen af sms- og e-mail-advisering og servicebeskeder fra offentlige afsendere via NemSMS til de anførte modtagere, jf. § 4, stk. 4. Digitaliseringsstyrelsen sletter ikke de i § 3 nævnte personoplysninger, da meddelelserne efter levering er overgået til modtagernes råde- og ejendomsret.	Digital Post og databehandleraftale med underleverandøren.		
Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolaktiviteter	Udført test	Yderligere bemærkninger
9.2	§12 Sletning af personoplysninger for juridiske enheder (BEK nr 2020 af 29/10/2021) Digitaliseringsstyrelsens databehandling i medfør af denne bekendtgørelse ophører: 1) Ved tranmission og levering af meddelelser til de af de juridiske enheder anførte modtageres digitale postkasse. 2) Når den juridiske enhed ikke længere opbevarer egne meddelelser i Digital Post. Stk. 2. Digitaliseringsstyrelsen sletter ikke de i § 3 nævnte personoplysninger, da meddelelserne efter levering er overgået til modtagernes råde- og ejendomsret. Stk. 3. Digitaliseringsstyrelsen opbevarer de meddelelser, som modtagerne, en fysisk person eller en juridisk enhed, har i sin digitale postkasse, indtil modtageren selv vælger at slette meddelelsen fra sin digitale postkasse.	Ad stk. 1-3): Kontor for Digital Post har gennem databehandleraftalen med underleverandøren sikret, at sletning af personoplysninger følger denne bekendtgørelse. Kontor for Digital Post sikrer årligt, at denne aftale overholdes gennem kontrolmål i revisorerklæringerne fra underleverandøren i forbindelse med kontorets årlige tilsyn med Leverandøren.	Stk. 1-3) Der foreligger skriftlige krav og procedurer til underleverandøren af Digital Post, om opbevaring og sletning af de personoplysninger, som Digitaliseringsstyrelsen opbevarer på vegne af de juridiske enheder, samt hvordan denne sletning skal foregå, herunder ift. opfølgning på sletning. Det er reguleret i databehandleraftalen med underleverandøren. Procedurer om opbevaring og sletning og opdateres en gang om året. Revisionserklæringer er indhentet og revisionsbemærkninger i Netcompanys revisionserklæring er gennemgået.	N/A

Digitaliserings-
styrelsen