DIGITALISERINGSSTYRELSEN

Digital Post redegørelse om tilsyn med behandling af personoplysninger i 2022

August 2023

2023

Indhold

REDEGØRELSE 1. DEL

1. Indledning 4
1.1 Lovgrundlag 4
1.2 Om redegørelse for tilsyn med Digital Post 4

2. Ledelsens udtalelse og konklusion 5
2.1 Ledelsens udtalelse 5
2.2 Konklusion 5

3. Oplysningspligt og tilsynsmateriale 6
3.1 Oplysningspligt 6
3.2 Tilsyn og dokumentationsmateriale 7
3.3 Udvikling af redegørelsen og tilsynsmateriale 7
3.4 Kontaktoplysninger 7

REDEGØRELSE 2. DEL

4. Beskrivelsen af løsning og behandling af personoplysninger i Digital Post 9
4.1 Systembeskrivelse af løsningen Digital Post 9
4.2 Dataansvarskonstruktion og kategorier af personoplysninger 10
4.3 Risikovurdering, konsekvensanalyse og notat om risici 12
4.4 Overførsel uden for Danmark 13
4.5 Opbevaring og sletning af oplysninger 13
4.6 Tredjepartsleverandører og underdatabehandlere 14
4.7 Underretning om brud på persondatasikkerheden 14

5. Beskrivelse af tilsynets omfang 15
5.1 Formålet med tilsyn med behandling af personoplysninger i Digital Post 15
5.2 Tilsynets omfang og afgrænsning 15
5.3 Underleverandør til driftsløsningen Digital Post 16
5.4 Rigsrevisionen og Datatilsynet 16
5.5 Departementets koncern it-tilsyn 16

6. Metode og kontrolmål for det gennemførte tilsyn 18
6.1 Metode 18
6.2 Katalog med kontrolmål 19
6.3 Supplerende informationer og dokumentation 19

Bilag: Digital Post kontrolkatalog med tilsyn for perioden 2022 23

REDEGØRELSE 1. DEL

Indledning og ledelsens udtalelse samt konklusion om tilsyn med Digital Post

1. Indledning

Lovgrundlag, tilsynspligt og ansvar for afgivelse af redegørelse for tilsyn med behandling af personoplysninger i Digital Post for perioden 2022.

1.1 Lovgrundlag

Digitaliseringsstyrelsen har ifølge LBK nr. 686 af 15. april 2021 om Digital Post fra offentlige afsendere om Digital Post (herefter Digital Post-loven)[1] ansvaret for udvikling, drift, vedligeholdelse og forvaltning af Danmarks fællesoffentlige digitale postløsning, Digital Post. Både løsningen og beskederne hedder Digital Post.

Digital Post-lovens § 2a, stk. 5, om regler, ansvar og opgaver og tilsyn, er udmøntet i 2 bekendtgørelser henholdsvis nr. 2019 og nr. 2020 af 29. oktober 2021 om ansvar, opgaver og tilsyn med behandling af personoplysninger i Digital Post (herefter bekendtgørelserne)[2]. Bekendtgørelserne fastlægger roller, ansvar og forpligtelser for personoplysninger i Digital Post mellem Digitaliseringsstyrelsen, som databehandler og henholdsvis de dataansvarlige offentlige afsendere og juridiske enheder (herefter virksomheder). Bekendtgørelserne er de retligt bindende aftaler mellem parterne og regulerer Digitaliseringsstyrelsens behandling af personoplysninger i Digital Post på vegne af de dataansvarlige.

Af bekendtgørelserne fremgår det, at Digitaliseringsstyrelsen skal føre tilsyn med behandling af personoplysninger i Digital Post på vegne af de dataansvarlige og udfærdige en årlig redegørelse om tilsynsindsatsen, jf. § 13, stk. 2. Endvidere fører Digitaliserings og Ligestillingsministeriets[3] departement tilsyn med Digitaliseringsstyrelsen som databehandler på vegne af de dataansvarlige. Departementet udarbejder i den forbindelse en årlig tilsynsrapport, der udgør det databeskyttelsesretlige tilsyn de dataansvarlige kan føre med Digitaliseringsstyrelsen.

1.2 Om redegørelse for tilsyn med Digital Post

Digitaliseringsstyrelsen har i 2023 gennemført tilsyn med behandling af personoplysninger i Digital Post for perioden 2022 på vegne af de dataansvarlige offentlige afsendere og virksomheder. Denne redegørelse er udfærdiget af Digitaliseringsstyrelsens kontor med ansvar for tilsynsopgaver og udgør en skriftlig fremstilling af det udførte tilsyn.

Hensigten med redegørelsen er at stille de nødvendige oplysninger til rådighed for de dataansvarlige for at påvise overholdelse af regler i den europæiske og danske databeskyttelsesret.

---

[1] LBK nr. 686 af 15. april 2021 Bekendtgørelse af lov om Digital Post fra offentlige afsendere om Digital Post
[2] 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.
[3] Grundet ressortomlægningen den 15. december 2022 er Digitaliseringsstyrelsen overført fra Finansministeriet til Digitaliserings og Ligestillingsministeriet.

Redegørelsens første del indledes med en udtalelse fra Digitaliseringsstyrelsens ledelse og en sammenfattende konklusion for det årlige tilsyn med behandling af personoplysninger i Digital Post. I tilknytning til første del følger informationer om Digitaliseringsstyrelsens oplysningspligt og tilsynsmateriale, der stilles til rådighed for de dataansvarliges eget tilsyn med Digital Post.

Den anden del af redegørelsen omhandler det bagvedliggende arbejde og de handlinger, der har indgået i tilsynsindsatsen med Digital Post. Herunder beskrives it-systemløsningen, dataansvarskonstruktion og rammerne for tilsynsaktiviteter samt de gennemførte kontroller med personoplysninger i Digital Post. Resultaterne fra tilsynet fremgår af en skemaoversigt indsat i bilag til redegørelsen.

2. Ledelsens udtalelse og konklusion

Ledelsens udtalelse og sammenfattende konklusion på Digitaliseringsstyrelsens tilsyn med behandling af personoplysninger i Digital Post.

2.1 Ledelsens udtalelse

Den sammenfattende konklusion for perioden 2022 er udformet på grundlag af de forhold, der er beskrevet i denne redegørelse om Digital Post til de dataansvarlige offentlige afsendere og virksomheder.

Ledelsen bekræfter, at 2023 redegørelsen er udfærdiget af Digitaliseringsstyrelsen og retvisende beskriver konklusionen for det gennemførte tilsyn med behandling af personoplysninger i Digital Post for perioden 2022.

2.2 Konklusion

Tilsynet vurderer, at Digitaliseringsstyrelsen som ansvarlig for Digital Post har overholdt de databeskyttelsesretlige regler for behandling af personoplysninger, som er pålagt efter den europæiske databeskyttelsesforordning[4] og danske databeskyttelseslov[5]. Det overordnede billede viser, at der er etableret organisatorisk ledelse med informations- og persondatasikkerhed i Digitaliseringsstyrelsen samt styring af de forvaltningsmæssige opgaver med drift, udvikling og vedligeholdelse af Digital Post.

Konklusionen bygger på tilsynets samlede indtryk fra observationer, forespørgsler og forelagt materiale i tilknytning til 68 kontrolmål for Digitaliseringsstyrelsens opfyldelse af de forpligtelser, der fremgår af bekendtgørelserne om Digital Post.

Det gennemførte tilsyn viser, at Digitaliseringsstyrelsen har etableret relevante politikker, processer, tekniske og sikkerhedsmæssige foranstaltninger ved behandling af

[4] Europa-Parlamentets og Rådets forordning af 2016-04-27 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (2016/679).
[5] LOV nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

personoplysninger i Digital Post. Ligeledes viser tilsynet også, at Digitaliseringsstyrelsen har løst ansvaret for de administrative opgaver med opfølgning på it-kontraktkrav, instruks i databehandleraftale og regler i bekendtgørelserne om Digital Post.

Digitaliseringsstyrelsen har fremlagt dokumentation for blandt andet revisionserklæringer for 2022 uden anmærkninger fra hovedleverandøren af Digital Post, og de interne forretningsgange der berører relevante emner omkring persondatasikkerhed, herunder håndtering af sikkerhedshændelser.

For så vidt angår hændelseshåndtering har Digitaliseringsstyrelsen registreret 10 brud på persondatasikkerheden i perioden omkring leverandørskift af Digital Post i 2022. Hændelserne er anmeldt til Datatilsynet, som aktuelt har afsluttet behandling af 7 anmeldelser med besked om, at der ikke er grundlag for at foretage sig yderligere over for Digitaliseringsstyrelsen.

Afslutningsvis skal det fremhæves, at der udestår mindre justeringer af informationssikkerhedsmaterialet og de administrative procedurer i Digitaliseringsstyrelsen. Det er dog tilsynets opfattelse, at de udestående justeringer er af organisatorisk karakter, og overvejende hænger sammen med indføring af bekendtgørelserne og etablering af Digitaliseringsstyrelsen under nyt ministerområde i 2022.

3. Oplysningspligt og tilsynsmateriale

Oplysningspligt om behandling af personoplysninger og offentliggørelse af information omkring Digital Post samt tilhørende tilsynsmateriale.

3.1 Oplysningspligt

Ved behandling af personoplysninger i Digital Post er der oplysningspligt til de dataansvarlige offentlige afsendere og virksomheder. For at informere bredt til myndigheder, borgere og virksomheder og samtidigt skabe gennemsigtighed har Digitaliseringsstyrelsen offentliggjort informationer om løsningen Digital Post.

Informationerne kan tilgås på Digitaliseringsstyrelsens hjemmeside og omhandler blandt andet retsgrundlag, dataansvar, opbevaring, sletning, leverandører, rettigheder og tilsyn i forbindelse med drift, vedligeholdelse og forvaltning af Digital Post. Informationerne bliver løbende vedligeholdt, så alle oplysningerne til enhver tid er aktuelle.

I denne redegørelse er der desuden medtaget en række relevante informationer omkring it-arkitekturløsningen og dataansvarskonstruktionen for behandling af personoplysninger, som er væsentlige til forståelsen af tilsynsindsatsen med Digital Post.

På Digitaliseringsstyrelsens hjemmeside digst.dk under menuen "It-løsninger" og punktet "Digital Post" findes nedenstående hovedemner med informationer om Digital Post.

- Om løsningen
- Lovgivning
- Anvendelse
- Vejledning
- Kommunikationsmateriale
- Netværk om Digital Post
- Support
- Tilsyn

3.2 Tilsyn og dokumentationsmateriale

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

- Digitaliserings- og Ligestillingsministeriets departements 2023 tilsynsrapport om Digitaliseringsstyrelsens tilsynspligt med behandling af personoplysninger i Digital Post
- Digitaliseringsstyrelsens 2023 redegørelse om tilsyn med behandling af personoplysninger i Digital Post for perioden 2022
- Notat om risici ved Digitaliseringsstyrelsens behandling af personoplysninger som databehandler
- Revisionserklæringer om Digital Post for perioden 2022 fra Digitaliseringsstyrelsens underleverandør.

3.3 Udvikling af redegørelsen og tilsynsmateriale

Udarbejdelse af denne redegørelse er den første efter ikrafttrædelse af bekendtgørelserne om Digital Post i november 2021. Udformningen af redegørelsen og tilhørende tilsynsmateriale vil derfor de kommende år blive tilpasset i takt med de dataansvarliges behov for indsigt i de udførte tilsynshandlinger.

3.4 Kontaktoplysninger

Ved henvendelser om overholdelse af de generelle regler om behandling af personoplysninger inden for ministerområdet er der mulighed for at kontakte Digitaliserings- og Ligestillingsministeriets databeskyttelsesrådgiver.

For så vidt angår specifikke spørgsmål til Digital Post vedrørende behandling af personoplysninger eller andet, så kontakt Digitaliseringsstyrelsens kontor med ansvar for Digital Post.

Digitaliserings- og Ligestillingsministeriet
Generelle henvendelse om regler og rettigheder i forbindelse med behandlingen af personoplysninger inden for ministerområdet kan rettes til databeskyttelsesrådgiveren på e-mail: dpo@digst.dk.

Digitaliseringsstyrelsens "Kontor for Digital Post"
Specifikke henvendelser vedr. oplysningspligt om behandling af personoplysninger i Digital Post og redegørelse for tilsyn samt materiale kan ske på e-mail: digitalpost@digst.dk.

REDEGØRELSE 2. DEL

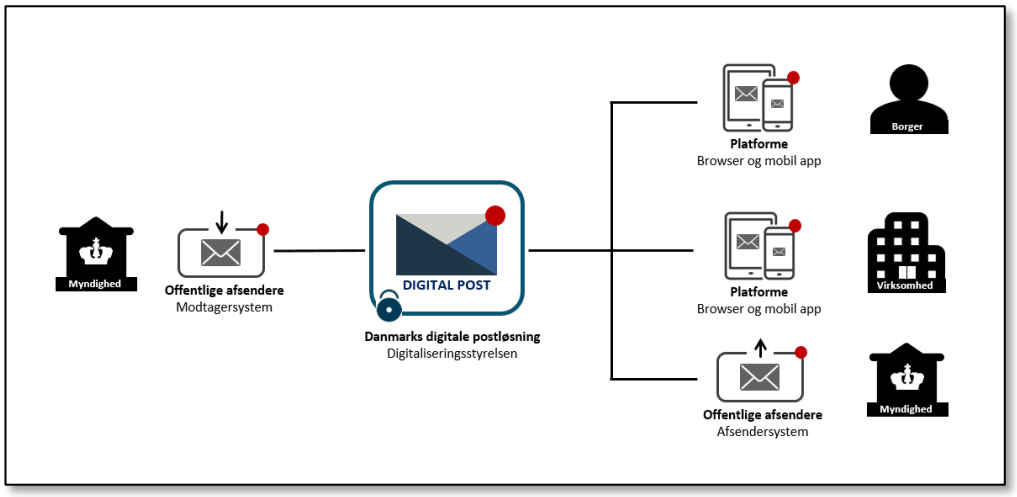
Systembeskrivelse, baggrund, omfang og tilsynsindsats med Digital Post

4. Beskrivelsen af løsning og behandling af personoplysninger i Digital Post

Beskrivelse af løsningen Digital Post og aktiviteter som indgår i Digitaliseringsstyrelsens behandling samt tilsyn med personoplysninger i Digital Post.

4.1 Systembeskrivelse af løsningen Digital Post

Nedenstående tegning viser sammenhæng og funktioner i it-arkitekturløsning for Digital Post. Den grafiske tegning illustrerer, at Digital Post sendes gennem ét system og kan derefter tilgås gennem flere platforme; fx browser eller mobil app til kommunikation mellem offentlige myndigheder, borgere og virksomheder. Dette kunne eksempelvis være Digital Post sendt fra kommuner, Skat og hospitaler via Digital Post.



Nedenstående tekstboks indeholder en kort forklaring af dataansvarskonstruktion og rollefordeling mellem myndigheder, virksomheder og Digitaliseringsstyrelsen samt de digitale platforme (visningsklienter).

Kort forklaring af dataansvarskonstruktion
Offentlige myndigheder er dataansvarlige for indholdet af postmeddelelser, de sender gennem Digital Post, og desuden dataansvarlig for modtagelse samt opbevaring af postmeddelelser i myndighedens eget modtagersystem. Digitaliseringsstyrelsen er databehandler for forsendelsen af meddelelser og dataansvarlig for administrationsdata i den driftstekniske del af Digital Post.

Virksomheder er dataansvarlige for indholdet af de postmeddelelser, de sender og opbevarer ved hjælp af Digital Post. Digitaliseringsstyrelsen er databehandler for forsendelse samt opbevaring af meddelelser i virksomhedernes postkasser i Digital Post og dataansvarlig for administrationsdata i den driftstekniske del af Digital Post.

De digitale platforme består af en række offentlige og kommercielle visningsklienter såsom Digital Post app, Borger.dk, Virk.dk, e-Boks og Mit.dk. Ved brug af en browser eller mobil app kan en borger eller virksomhed læse sine postmeddelelser fra offentlige myndigheder eller virksomheder. Udbydere af visningsklienter er selvstændige dataansvarlige for platformene men ikke dataansvarlig for personoplysninger indeholdt i meddelelser, der er sendt fra offentlige afsendere.

4.2 Dataansvarskonstruktion og kategorier af personoplysninger

Indledningsvis skal det nævnes, at lov og bekendtgørelserne om Digital Post ikke frigør den dataansvarlige og databehandleren fra andre forpligtelser, som er pålagt efter databeskyttelsesforordningen, databeskyttelsesloven eller anden lovgivning.

De efterfølgende afsnit opridser dataansvarskonstruktion for personoplysninger ved forsendelse, opbevaring og indhold af postmeddelelser i Digital Post. En uddybende beskrivelse af dataansvarskonstruktion for borgere, myndigheder, virksomheder og visningsklientudbydere findes på Digitaliseringsstyrelsens hjemmeside.

Digitaliseringsstyrelsens formål med behandling af personoplysninger

Jf. § 2 a i Digital Post-loven er Digitaliseringsstyrelsen dataansvarlig for behandling af personoplysninger til formål, der omhandler levering af meddelelser, vedligeholdelse, udvikling og forvaltning af den driftstekniske fællesoffentlige løsning til Digital Post.

Behandlingen af almindelige personoplysninger vedrører borgere, virksomheder og medarbejdere i forbindelse med de drifts- og systemtekniske opgaver. Digitaliseringsstyrelsen registrerer og viser nødvendige informationer om, hvornår en postmeddelelse er sendt, hvem der er afsender og modtager af meddelelsen.

Indsamling og kategorier af personoplysninger

Digitaliseringsstyrelsen indsamler personoplysninger fra blandt andet CVR-registret og Statstidende og behandler almindelige personoplysninger såsom personnumre, CVR-numre, e-mail og telefonnumre eller lignende, jf. § 2 a i Digital Post-loven. Indsamling og behandling af nedenstående almindelige personoplysninger i Digital Post sker i forbindelse med forvaltning af administrationsdata i den driftstekniske del af Digital Post:

- Fornavn
- Efternavn
- Personnummer
- Adresse
- E-mailadresse
- Telefonnummer
- Hændelser og handlinger om virksomheden i Digital Post
- UUID (Tilfældigt genereret identifikationsnummer)
- CVR-nummer (Kun virksomheder)

Offentlige afsendere som dataansvarlige og Digitaliseringsstyrelsen som databehandler

De offentlige afsendere er dataansvarlige for indholdet af de postmeddelelser, de sender via Digital Post, og Digitaliseringsstyrelsen er databehandler for forsendelsen af meddelelser, jf. § 2 a, stk. 3 i Digital Post-loven.

Digitaliseringsstyrelsens rolle som databehandler for offentlige afsenderes forsendelse af meddelelserne indebærer, at styrelsen alene behandler personoplysninger indeholdt i postmeddelelserne iht. instruks, der er reguleret i bekendtgørelserne

om Digital Post. Digitaliseringsstyrelsen har således ikke indflydelse på, hvornår postmeddelelser er afsendt eller indholdet af meddelelserne.

Offentlige afsendere er pålagt oprettelse af eget system til modtagelse ("modtagersystemer") og opbevaring af postmeddelelser, som bevirker at Digitaliseringsstyrelsen ikke er databehandler for opbevaringen, jf. § 2 a i Digital Post-loven og de specielle bemærkninger til denne bestemmelse i § 1, nr. 2 i forslag til lov om ændring (herefter Digital Post-lovforslag)[6].

Virksomheder som dataansvarlige og Digitaliseringsstyrelsen som databehandler
De juridiske enheder (herefter "virksomheder") er dataansvarlige for indholdet af meddelelser, de sender og opbevarer via Digital Post. Digitaliseringsstyrelsen er databehandler for virksomhedernes forsendelse og opbevaring af meddelelser i virksomhedens digitale postkasse, der udgør en del af den digitale postløsning, jf. § 2 a, stk. 4, 2. sætning i Digital Post-loven.

Efter modtagelse af digitale postmeddelelser vil borgere og virksomheder være de eneste med råde- og ejendomsret over egen Digital Post, jf. de almindelige bemærkninger i afsnit 2.2.2 i Digital Post-lovforslag. Digitaliseringsstyrelsen er derfor ikke databehandler for opbevaring af posten i borgerens egen digitale postkasse.

Virksomheder, som modtager Digital Post indeholdende oplysninger om fx kunder eller medarbejdere, er derimod dataansvarlige for de personoplysninger, der opbevares i den digitale postkasse. Opbevaringen varetages af Digitaliseringsstyrelsen som databehandler.

Borgere har råde- og ejendomsret
Databeskyttelsesforordningen finder ikke anvendelse for behandling af personoplysninger, som foretages af en fysisk person som led i rent personlige eller familiemæssige aktiviteter. Borgere er dermed ikke i databeskyttelsesretlig forstand dataansvarlige for den digitale post i egen digitale postkasse, uanset om posten måtte indeholde personoplysninger om tredjeparter, jf. de almindelige bemærkninger i afsnit 2.2.2 i Digital Post-lovforslag.

Visningsklienter som dataansvarlig
De såkaldte visningsklienter er en digital platform, hvor en borger eller virksomhed ved hjælp af en browser eller mobil app, kan få vist sin digitale post fra offentlige myndigheder. Her skelnes henholdsvis mellem to former for visningsklienter: offentlige og kommercielle. De offentlige platforme herunder Digital Post app, Borger.dk og Virk.dk, fungerer som klienter for visning af postmeddelelser fra offentlige myndigheder. De kommercielle platforme, e-Boks og Mit.dk, fungerer som klienter for visning af Digital Post fra både offentlige myndigheder og private virksomheder.

Udbydere af både offentlige og kommercielle visningsklienter er selvstændigt dataansvarlige for deres behandling af personoplysninger, som er nødvendig for at en

---

[6] Lovforslag nr. 47, fremsat den 8. oktober 2020 om ændring af lov om Digital Post fra offentlige afsendere (Hjemtagelse til Digitaliseringsstyrelsen af dataansvar, strategisk ejerskab og beslutningskompetence for Digital Post, etablering af visningsklienter og flytning af borgeres og virksomheders post)

borger eller virksomhed kan få vist sine postmeddelelser. De pågældende udbydere af visningsklienter vurderer, hvilke personoplysninger de finder nødvendige at behandle i forbindelse med de tekniske foranstaltninger ved drift, vedligeholdelse og administration af deres visningsklient; fx navn, e-mails og telefonnumre jf. § 10, stk. 3 i bekendtgørelse nr. 331 af 16. marts 2022 om godkendelse af visningsklienter til Digital Post (Herefter visningsklient-bekendtgørelsen)[7].

Visningsklientudbyderen er ikke dataansvarlig for personoplysninger indeholdt i meddelelserne, der er sendt fra offentlige afsendere.

4.3 Risikovurdering, konsekvensanalyse og notat om risici

Digitaliseringsstyrelsen har udarbejdet en risikovurdering for Digital Post, og på baggrund af identificerede risici fastlagt et sikkerhedsniveau for implementering af tekniske samt organisatoriske foranstaltninger.

I medfør af bekendtgørelserne § 6, stk 1 skal der stilles en sammenfatning af den foretaget risikovurderingen til rådighed for de dataansvarlige. Med afsæt i resultaterne fra risikovurderingen af Digital Post har Digitaliseringsstyrelsen udarbejdet et selvstændigt notat om risici til de dataansvarlige, som offentliggøres. Notatet er udformet, så der tages hensyn til at Digital Post er et samfundskritisk infrastruktursystem i Danmark.

Endvidere har Digitaliseringsstyrelsen i samarbejde med Kammeradvokaten udarbejdet en konsekvensanalyse i rollen som dataansvarlig for personoplysninger i Digital Post. Formålet med analysen er at identificere og evaluere risici, samt at pege på implementering af mulige begrænsende foranstaltninger i forbindelse med brugen af Digital Post.

Resultatet af konsekvensanalysen viser, at den samlede risiko forbundet med behandlingen af personoplysninger i Digital Post er *mellem*. Det betyder, at konsekvensen ved en risiko indtræffer er nedbragt til *mellem* efter indførelse af tekniske og organisatoriske sikkerhedsforanstaltninger. Konsekvensanalysen er ikke sendt i høring hos Datatilsynet, eftersom behandlingen ikke vil føre til *høj* risiko for de registrerede jf. databeskyttelsesforordningens artikel 36, stk. 1.

Digitaliseringsstyrelsen har i forbindelse med udarbejdelse af konsekvensanalysen identificeret en række risici i rollen som databehandler på vegne af de dataansvarlige. I tidligere nævnte notat om risici har Digitaliseringsstyrelsen med afsæt i risikovurdering og konsekvensanalysen af Digital Post listet forskellige scenarier af identificerede risici, som er forbundet med behandling af personoplysninger. Håndtering og begrænsning af de pågældende scenarier er beskrevet i en skemaoversigt for henholdsvis Digitaliseringsstyrelsen og de dataansvarlige.

Digitaliseringsstyrelsens notat om risici kan benyttes af de dataansvarlige i deres videre arbejde med egne konsekvensanalyser af Digital Post, herunder valg af foranstaltninger til mulige begrænsning af risici, såfremt det vurderes nødvendigt. Notat om risici kan hentes på Digitaliseringsstyrelsens hjemmeside.

---

[7] Bekendtgørelse nr. 331 af 16. marts 2022 om godkendelse af visningsklienter til Digital Post samt kompensation for forpligtelser til offentlig tjeneste for udbydere af kommercielle visningsklienter.

4.4 Overførsel uden for Danmark

I medfør af bekendtgørelse om lokationskrav nr. 220 af 11. februar 2022 (herefter lokationskravsbekendtgørelsen)[8] har Justitsministeriet vurderet, at den digitale postløsning i sin helhed er særlig kritisk for samfundet og ved behandling af personoplysninger uden for Danmarks grænser. Resultatet af vurderingen indebærer dermed en risiko for statens sikkerhed, og Digital Post er derfor omfattet af lokationskravet om personoplysninger i henholdt til databeskyttelsesloven.

It-systemer der er omfattet af databeskyttelseslovens § 3, stk. 9 er omfattet af lokationskravet. I denne sammenhæng betyder lokationskravet, at de kritiske dele af Digital Post driftsløsningen ikke må placeres uden for Danmarks grænser. De ikke-kritiske dele af driftsløsningen såsom vedligeholdelses- og supportfunktioner kan eventuelt placeres uden for Danmark efter skriftlig godkendelse af Digitaliseringsstyrelsen.

4.5 Opbevaring og sletning af oplysninger

Der er fastlagt tidsfrister for sletning af de opbevarede oplysninger om borgere og virksomheder. Nedenfor er listet tidsfrister for opbevaring og sletning af oplysninger for postmeddelelser i Digital Post:

- Oplysninger om borgeren slettes 5 år efter død
- Oplysninger om virksomheder behandles indtil 10 år efter ophør af virksomheden, hvorefter oplysningerne slettes
- Oplysninger vedrørende hændelser i Digital Post; fx modtagelse af en postmeddelelse, opbevares op til 2 år, hvorefter de slettes

Udover ovennævnte frister kan borgere og virksomheder altid selv slette postmeddelelser i den digitale postkasse.

Sletning af personoplysninger for offentlige afsendere

I medfør af bekendtgørelsen om Digital Post for offentlige afsendere § 12 ophører Digitaliseringsstyrelsens databehandling ved levering af sms- og e-mail-advisering samt servicebeskeder fra offentlige afsendere fra NemSMS til de anførte modtagere. Digitaliseringsstyrelsen sletter derfor ikke de omfattede personoplysninger i forbindelse med sin behandling, da meddelelserne efter levering er overgået til modtagernes råde- og ejendomsret.

Sletning af personoplysninger for virksomheder

Det fremgår endvidere af § 12, stk. 1-3 i bekendtgørelsen om Digital Post for virksomheder, at Digitaliseringsstyrelsens databehandling ophører:

1) Ved transmission og levering af meddelelser til virksomhedernes anførte modtageres digitale postkasse
2) Når virksomheder ikke længere opbevarer egne meddelelser i Digital Post

Digitaliseringsstyrelsen sletter ikke de omfattede personoplysninger, da meddelelserne efter levering er overgået til modtagernes råde- og ejendomsret. Det bevirker,

[8] BEK nr. 220 af 11. februar 2022 Bekendtgørelse om hel eller delvis opbevaring her i landet af personoplysninger, der behandles i nærmere bestemte it-systemer, og som føres for den offentlige forvaltning

at Digitaliseringsstyrelsen opbevarer meddelelser i de digitale postkasser, indtil borgerne eller virksomhederne vælger at slette meddelelsen fra sin digitale postkasse.

4.6 Tredjepartsleverandører og underdatabehandlere

Digitaliseringsstyrelsen har indgået it-kontrakter og tilslutningsaftaler med tredjepartsleverandører, der leverer it-driftsydelser til løsningen 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.

I tilknytning til leverandørsamarbejdet har Digitaliseringsstyrelsen indgået underdatabehandleraftaler med henblik på at overholde regler om persondatabeskyttelse og sikre privatlivets fred samt fysiske personers grundlæggende rettigheder.

For så vidt angår både offentlige og kommercielle underleverandører af Digital Post platforme er udbyderne selvstændigt dataansvarlige for deres behandling af personoplysninger i visningsklienterne, jf. afsnit 4.2.

Det praktiske arbejde med systemforvaltning og det årlige tilsyn med underleverandører løftes gennem det løbende samarbejde mellem Digitaliseringsstyrelsen og de pågældende underleverandører. De indgåede it-kontrakter og databehandleraftaler regulerer forpligtelser samt de nærmere vilkår for leverandørsamarbejdet.

Gennemførelsen af det formelle leverandørtilsyn bygger på de årlige revisionserklæringer om sikkerhed og GDPR, der er afgivet af underleverandørerne. Revisionserklæringerne er udarbejdet af uafhængige statsautoriserede revisorer og omfatter revisionskontroller og test med underleverandørernes driftsydelser samt foranstaltninger til persondatasikkerhed iht. kontraktkrav og databehandleraftaler.

De dataansvarlige 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 revisionserklæringer fra underdatabehandlere til rådighed for de dataansvarlige offentlige afsendere og virksomheder på Digitaliseringsstyrelsens hjemmeside.

4.7 Underretning om brud på persondatasikkerheden

Der er etableret procedurer for rapportering, registrering og håndtering af opfølgning på brud eller forsøg på misbrug af informations- og persondatasikkerheden internt i Digitaliseringsstyrelsen og hos underdatabehandlere.

Digitaliseringsstyrelsen har aftalt de juridiske forpligtelser for underretning og tidsfrister for meddelelse om eventuelle sikkerhedsbrud til Digitaliseringsstyrelsen, de dataansvarlige samt indberetning til Datatilsynet.

5. Beskrivelse af tilsynets omfang

Beskrivelse af formål, omfang og rammerne for Digitaliseringsstyrelsens tilsyn med behandling af personoplysninger i Digital Post.

5.1 Formålet med tilsyn med behandling af personoplysninger i Digital Post

Digitaliseringsstyrelsen har en rolle som henholdsvis databehandler og dataansvarlig i relation til behandling af personoplysninger i Digital Post. Formålet med tilsynet er derfor at undersøge, hvorvidt Digitaliseringsstyrelsen har etableret en betryggende styring og tilrettelagt en hensigtsmæssig systemforvaltning af Digital Post i overensstemmelse med de databeskyttelsesretlige forpligtelser.

I praksis betyder det, at tilsynet skal tilse og vurdere, om beskyttelsen af personoplysninger og den tilhørende informationssikkerhed i Digital Post foregår pålideligt og sikkerhedsmæssigt forsvarligt, så oplysningernes fortrolighed, integritet og tilgængelighed sikres i nødvendigt omfang.

Grundlaget for tilsynet er de forpligtelser, der fremgår af reglerne i bekendtgørelserne om databehandling af personoplysninger for offentlige afsendere og virksomheder i Digital Post. Reglerne er udformet inden for rammerne af EU databeskyttelsesforordning og databeskyttelsesloven om supplerende bestemmelser til forordningen.

5.2 Tilsynets omfang og afgrænsning

Tilsynet tager afsæt i Digitaliseringsstyrelsens forpligtelser til styring af personoplysninger og den understøttende informationssikkerhed, som påhviler ved behandling af personoplysninger i Digital Post på vegne af de dataansvarlige jf. Digital Post-loven og bekendtgørelserne.

Omfanget af tilsynet dækker Digitaliseringsstyrelsens interne organisatoriske ledelsesstyring med informationssikkerhed og behandling af personoplysninger relateret til Digital Post. Hertil hører ansvaret for kontraktstyring af underleverandører og tilhørende løsning af de løbende forvaltningsmæssige opgaver med udvikling, drift og vedligeholdelse af Digital Post hos underleverandører.

Det betyder, at tilsynet, foruden tilsyn med den interne styring af informations- og persondatasikkerhed, har fokus på Digitaliseringsstyrelsens leverandørstyring. Tilsynet omhandler derfor også forpligtelser i forhold til de administrative og forvaltningsmæssige opgaver med opfølgning på kontraktkrav, driftsydelser og revisionsbevis for overholdelse af reglerne om beskyttelse af personoplysninger hos underleverandører.

Hertil kommer, at tilsynet ligeledes omfatter indhentning af supplerende informationer, der berører relevante sikkerhedsemner omkring behandling af personoplysninger i Digital Post. Hensigten med dette er at opnå et fyldestgørende vurderingsgrundlag af Digitaliseringsstyrelsens varetagelse af persondatabeskyttelse og den understøttende informationssikkerhed.

Tilsynsarbejdet indbefatter således også de forpligtelser, der påhviler Digitaliseringsstyrelsen til overholdelse af informationssikkerhed efter ISO 27001 standarden, tilsynspligt med underleverandører og indhentning af revisionserklæringer. Desuden inddrages konklusionen fra departementets ministerielle koncern it-tilsyn og eventuelle undersøgelser udført af Rigsrevisionen samt anmeldelser til Datatilsynet.

5.3 Underleverandør til driftsløsningen Digital Post

Digitaliseringsstyrelsen er som nævnt ansvarlig for udvikling, drift, vedligeholdelse og forvaltning af Danmarks fællesoffentlige digitale postløsning i henhold til Digital Post-loven.

I 2019 var der lovpligtig udbud af driftsopgaven med Digital Post til sikker digital kommunikation mellem myndigheder, borgere og virksomheder. Udbuddet som hovedleverandør af Digital Post blev vundet af Netcompany, og overgangen til en ny Digital Post blev lanceret den 21. marts 2022.

Nedenfor er listet de udpegede underleverandører, der varetager hoved- eller delopgaver i forbindelse med drift, udvikling og support af Digital Post. Listen med leverandører findes også på Digitaliseringsstyrelsens hjemmeside.

- Netcompany A/S varetager hovedopgaverne vedrørende drift, vedligeholdelse og videreudvikling af Digital Post
- Fellowmind Denmark A/S varetager it-udviklingsopgaver af Digital Post
- Erhvervsstyrelsen løser brugersupportopgaver om Digital Post til borgere og virksomheder
- Statens It varetager visse driftsopgaver i Digital Post

Hovedleverandøren Netcompany er ansvarlig for, at behandling af personoplysninger, som finder sted i forbindelse med driftsløsningen af Digital Post, sker inden for rammerne af databeskyttelsesforordningen og databeskyttelsesloven. Som en del af forvaltningsopgaverne med Digital Post er Digitaliseringsstyrelsen tilsynsansvarlig og gennemfører et årligt leverandørtilsyn med Netcompany.

Digitaliseringsstyrelsens tilsyn med underleverandørens efterlevelse af informationssikkerhed og persondatabeskyttelse bygger på de årlige revisionserklæringer, der er afgivet af Netcompany. Revisionserklæringerne er udarbejdet af uafhængige statsautoriserede revisorer i henhold til indgået it-kontraktkrav om sikkerhed, revision og instruks i databehandleraftale for Digital Post.

5.4 Rigsrevisionen og Datatilsynet

Digitaliseringsstyrelsens er underlagt Folketingets uafhængige institutioners parlamentariske kontrol i Danmark og indgår derfor i de løbende undersøgelser af Rigsrevisionen og Datatilsynet. Den parlamentariske kontrol understøtter således en uafhængig revision og tilsyn med Digitaliseringsstyrelsens forvaltning, tilsynspligt, overholdelse af love og informationssikkerhed samt persondatabeskyttelse.

5.5 Departementets koncern it-tilsyn

Digitaliseringsstyrelsen er ydermere underlagt et ministerielt årligt koncernrettet it-tilsyn af Digitaliserings- og Ligestillingsministeriets departement. På ministerområdet gennemfører departementet et it-tilsyn med Digitaliseringsstyrelsen og øvrige

underliggende styrelser samt eventuelle statslige virksomheder. Departementets koncerntilsyn har til formål, at give en uafhængig og overordnet vurdering af den ledelsesmæssige styring af forretningsgange og kontroller med it-sikkerheden og persondatabeskyttelse i Digitaliseringsstyrelsen.

Departementet afgiver en årlig koncernrapport 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.

6. Metode og kontrolmål for det gennemførte tilsyn

Beskrivelse af metode for det praktiske tilsyn og tilhørende kontrolmål som grundlag for tilsyn med behandling af personoplysninger i Digital Post.

6.1 Metode

Tilsynet med Digitaliseringsstyrelsens ledelsesstyring af informations- og persondatasikkerhed samt systemforvaltning af Digital Post hos underleverandøren gennemføres i dialog med det ansvarlige kontor for Digital Post i Digitaliseringsstyrelsen.

Til brug for gennemførsel af tilsynsaktiviteterne anvendes et arbejdsdokument i form af et kontrolkatalog (se bilag sidst i redegørelsen), som er udarbejdet i samarbejde mellem Digitaliseringsstyrelsen og Kammeradvokaten. Kontrolkataloget består af et skema med beskrivelse af regler for Digitaliseringsstyrelsens opfyldelse af myndighedsforpligtelser og tilhørende kontrolmål, som dækker reguleringen i bekendtgørelserne fra §§ 4-12 om Digital Post. Kataloget danner grundlaget for Digitaliseringsstyrelsens dokumentation for efterlevelse af de pågældende krav og etablering af procedurer samt dokumentation.

Det udførte tilsyn med kontrolkataloget dækker en kombination af de tre tilsynsmetoder; forespørgsel, observation og inspektion, som beskrevet i nedenstående skema.

Metode	Beskrivelse
Forespørgsel	Indhentning af information omhandlende beskrivelser af bestemte forretningsgange og tilhørende kontroller.
Observation	Overværelse af at fysiske eller digitale processer gennemføres, og hvordan de er etableret.
Inspektion	Gennemsyn og vurdering af dokumentation for, at bl.a. politikker, procedurer og kontroller overholdes.

Tilsynets vurderingsgrundlag for overholdelse af databeskyttelsesregler og sikkerhedsforanstaltninger i Digital Post bygger således på mundtlige forespørgsler om arbejdsgange, overværelse af hvordan forretningsprocesser fungerer i praksis og skriftlig dokumentation for overholdelse heraf.

Omfanget af tilsynsaktiviteter er tilrettelagt efter Digitaliseringsstyrelsens forpligtelser og ansvar med den ledelsesmæssige styring, administration og forvaltning af Digital Post. Udførsel af tilsynshandlinger med de skriftlige politikker og procedurer for kontrol af den digitale postløsning er opdelt på følgende 3 organisatoriske forretningsområder i Digitaliseringsstyrelsen:

1) Ledelsesstyring med informations- og persondatasikkerhed; fx overordnede politikker, retningslinjer og procedurer i organisationen
2) Kontor med ansvar for vedligeholdelse, udvikling og forvaltning af Digital Post
3) Leverandørstyring i henhold til it-kontraktkrav og underdatabehandleraftale om Digital Post med underleverandør

Udførelse, indhold og resultat af tilsynsindsatsen er kvalitetssikret med relevante fagkontorer i Digitaliseringsstyrelsen. Undervejs i tilsynsforløbet har der været løbende dialog med det ansvarlige kontor for Digital Post, der har bidraget med supplerende oplysninger og dokumentation til opfyldelse af kontrolmål ifølge kontrolkatalog. Det pågældende kontor har desuden afgivet kommentarer til udkast af den årlige redegørelse for tilsyn med Digital Post.

Ved udførelse af de nævnte tilsynsmetoder indgår der ikke tekniske test- eller kontrolhandlinger af procedurer, da dette hører under kontrolaktiviteter ved revision og auditering.

6.2 Katalog med kontrolmål

Kontrolkataloget består af en række punkter med fastlagte kontrolmål, der er udformet i henhold til regulering §§ 6-11 i bekendtgørelserne om Digital Post. Rammeværket for opstilling af kontrolmål dækker regulering af regler i §§ 4-12 og er udvalgt med bistand fra Kammeradvokaten ud fra en risikobaseret tilgang og med afsæt i standarderne for henholdsvis informationssikkerhed ISO 27001 og privatlivsbeskyttelse ISO 27701.

De enkelte kontrolmål er endvidere formuleret med afsæt i revisorernes skabelon for GDPR revisionserklæring, som er udarbejdet i samarbejde mellem Datatilsynet og "FSR - danske revisorer" samt med input fra Datatilsynets vejledningsmateriale.

Kataloget indeholder en skemaopstilling med 19 punkter og 68 tilhørende kontrolmål. De 19 punkter indeholder regler fordelt på §§ 4-12 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 er udfyldt og ledelsesgodkendt af det ansvarlige kontor for Digital Post. Kontrollerne dækker Digitaliseringsstyrelsens ledelsesstyring af informations- og persondatasikkerhed, de interne procedurer for systemforvaltning og leverandørstyring af Digital Post.

Resultatet af det afsluttede tilsyn med kontrolkataloget for perioden 2022 fremgår af bilaget sidst i redegørelsen.

6.3 Supplerende informationer og dokumentation

For at styrke tilsynsindsatsen og vurderingsgrundlaget for Digitaliseringsstyrelsens behandling af personoplysninger samt den understøttende informationssikkerhed, er der indhentet supplerende informationer på en række områder.

For så vidt angår Rigsrevisionen og Datatilsynet foreligger der ikke oplysninger om gennemført revision eller tilsyn i perioden 2022, som berør Digitaliseringsstyrelsens behandling af personoplysninger i Digital Post.

I forlængelse af de nævnte 68 kontrolmål for tilsynsarbejdet med Digital Post er der nedenfor tilføjet uddybende informationer og status på tre centrale kontrolområder;

1) Brud på persondatasikkerhed
2) Leverandørstyring
3) Departementets koncern it-tilsyn

1) Status – brud på persondatasikkerheden
Digitaliseringsstyrelsen har i 2022 modtaget og registreret en række sikkerhedsbrud, som har haft betydning for behandling af personoplysninger i Digital Post. Hændelserne har alle været i perioden omkring lanceringen af den nye løsning af Digital Post i marts 2022.

I denne periode registrerede Digitaliseringsstyrelsen 10 hændelser, der omhandlede brud på persondatasikkerheden ved overgangen til den nye driftsleverandør af Digital Post. Hændelserne hang primært sammen med overførsel af data samt komplikationer med læseadgange og fuldmagter, som bevirkede at brugere ikke kunne tilgå Digital Post. I forbindelse med brugersupport og fejlsøgning af hændelserne blev Digitaliseringsstyrelsen opmærksom på, at materialet til fejlsøgning også kunne indeholde fortrolige oplysninger, hvorpå praksis blev stoppet.

Herudover har et antal brugere oplevet, at single sign-on stadig var aktivt, hvis de loggede ud fra en kommerciel postløsning og derefter tilgik eksempelvis borger.dk. Endelig konstaterede Digitaliseringsstyrelsen, at især udenlandsdanskere fejlagtigt blev tilmeldt Digital Post ved overførsel af tilmeldingsstatus til ny postløsning. Dette resulterede blandt andet i, at de ikke modtog leveattester per brev, vedrørende oplysninger om, hvorvidt borgeren er i live ved pensionsudbetaling.

I forlængelse af de nævnte hændelser har Digitaliseringsstyrelsen anmeldt 10 hændelser om brud på persondatasikkerheden til Datatilsynet, hvoraf 5 hændelser ikke er anmeldt inden for tidsfristen på 72 timer. Undervejs i hændelsesforløbet har Digitaliseringsstyrelsen straks begrænset skadesomfanget og sikret permanente løsninger for at undgå lignende fremtidige hændelser. Ydermere blev relevante borgere, myndigheder og virksomheder underrettet om hændelserne.

Datatilsynet har meddelt Digitaliseringsstyrelsen, at de har afsluttet behandling af 7 hændelser, og der ikke er grundlag for at foretage sig yderligere. Aktuelt udstår fortsat status fra Datatilsynet på 3 anmeldte brud på persondatasikkerheden i 2022.

2) Leverandørtilsyn med 2022 revisionserklæringer
Digitaliseringsstyrelsen har gennemført et separat leverandørtilsyn med Digital Post hos underleverandøren Netcompany. Det udførte tilsyn har fokuseret på Netcompanys efterlevelse af aftalte krav til informationssikkerhed og persondatabeskyttelse med driftsløsningen af Digital Post. Leverandørtilsynet med Netcompany har været baseret på de årlige revisionserklæringer for perioden 2022 i henhold til indgået it-kontraktkrav om sikkerhed, revision og instruks i databehandleraftale for Digital Post.

Netcompany har samlet set leveret 4 revisionserklæringer for perioden 2022, som er fordelt på to sæt erklæringer, der er adresseret til henholdsvis alle Netcompanys kunder og specifikt til Digitaliseringsstyrelsen for Digital Post.

2022 revisionserklæringerne for de generelle it-kontroller til kunderne
Revisionserklæringerne til kunderne dækker de generelle it-kontroller til driftsydelser samt de generelle sikkerhedsforanstaltninger til databeskyttelse og er udarbejdet for at opfylde almindelige behov for en bred kundekreds i Netcompanys driftsmiljø, herunder også dele af Digital Post driftsydelser.

2022 revisionserklæringer for de generelle it-kontroller:

- "Uafhængig revisors ISAE 3402 erklæring om generelle it-kontroller relateret til drifts- og hostydelser for perioden fra 1. januar 2022 til 31. december 2022"
- "Uafhængig revisors ISAE 3000 erklæring med sikkerhed om informationssikkerhed og foranstaltninger mod databeskyttelse samt behandling af personoplysninger. Erklæringen omfatter perioden fra 1. januar 2022 til 31. december 2022"

2022 revisionserklæringerne for Digital Post til Digitaliseringsstyrelsen
De specifikke revisionserklæringer til Digitaliseringsstyrelsen omhandler udvalgte it-kontroller om sikkerhed til driftsydelser og sikkerhedsforanstaltninger til databeskyttelse af personoplysninger i Digital Post systemløsning hos Netcompany.

2022 revisionserklæringer for udvalgte it-kontroller med Digital Post:

- "Uafhængig revisors ISAE 3402 type 2-erklæring om generelle it-kontroller relateret til Netcompanys ydelser på Næste Generations Digital Post leveret til Digitaliseringsstyrelsen for perioden fra 1. januar 2022 til 31. december 2022"
- "Uafhængig revisors ISAE 3000 type 2-erklæring med sikkerhed om udvalgte kontroller i tilknytning til informationssikkerhed og foranstaltninger mod databeskyttelse af personoplysninger relateret til Netcompanys ydelser på Næste Generations Digital Post leveret til Digitaliseringsstyrelsen for perioden fra 1. januar 2022 til 31. december 2022"

Tilsynet har noteret, at underleverandøren Netcompany i 2023 har leveret revisionsmateriale i henhold til aftalte formalia i it-kontrakt, databehandleraftale og udvalgte revisionskontroller jf. regulering i bekendtgørelserne om Digital Post. De årlige revisionserklæringer dækker perioden 1. januar 2022 til 31. december 2022 og er udfærdiget efter partielmetoden af det statsautoriserede revisionsselskab Deloitte.

Revisor har ikke konstateret mangler ved systemrevisionen, som har givet anledning til forbehold eller anmærkninger og dermed påvirket konklusionen af 2022 revisionserklæringerne. Revisors konklusion i de 4 leverede erklæringer viser således, at implementering og kontroller i alle væsentlige henseender er tilfredsstillende samt effektive for at give høj grad af sikkerhed.

3) Departementets koncern it-tilsyn med Digitaliseringsstyrelsen
Departementet har gennemført et årligt koncernrettet it-tilsyn med informationssikkerheden i Digitaliseringsstyrelsen for perioden 2022. Tilsynet omfattede de forpligtelser, der påhviler Digitaliseringsstyrelsen i forhold til styring af informationssikkerhed efter ISO 27001, efterlevelse af GDPR og opfølgning på bemærkninger fra revisions- og tilsynsmyndigheder.

I departementets 2022 tilsynsrapporten om Digitaliseringsstyrelsen konkluderes det overordnet, at Digitaliseringsstyrelsens modenhedsniveau er højt i forhold til compliance og effektivitet på de undersøgte områder. Endvidere fremgår det, at tilsynet med informationssikkerheden i Digitaliseringsstyrelsen ikke har givet anledning til væsentlige bemærkninger.

Bilag: Digital Post kontrolkatalog med tilsyn for perioden 2022

Tilsynsarbejdet med Digital Post for perioden 2022 tager udgangspunkt i et kontrolkatalog, der er udfyldt og ledelsesgodkendt af det ansvarlige kontor for Digital Post i Digitaliseringsstyrelsen. Kataloget består af et skema med 19 punkter og 68 tilhørende kontrolmål vedrørende Digitaliseringsstyrelsens forpligtelser i henhold til bekendtgørelserne om Digital Post for offentlige afsendere og juridiske enheder.

De 19 opstillede punkter og de 68 fastlagte kontrolmål er identificeret på baggrund af de forpligtelser, der fremgår af §§ 4-12 relateret til Digitaliseringsstyrelsens databehandling af personoplysninger i Digital Post jf. bekendtgørelserne.

§ 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

Nedenstående skemaoversigt er en kopi af kontrolkataloget, og indsat i en tilpasset form. Skemaet indeholder de 19 punkter med beskrivelse af forpligtelser og 68 kontrolmål med tilføjelse af tilsynets udførte test samt resultater. Skemaet udgør dokumentation for resultatet af det afsluttede tilsyn med Digital Post for perioden 2022.

Tilsynet er gennemført på baggrund af forespørgsler, observationer og inspektioner samt en vurdering af Digitaliseringsstyrelsens opfyldelse af kontrolmål. Omfanget af tilsynsaktiviteter er tilrettelagt efter Digitaliseringsstyrelsens forpligtelser og ansvar med den ledelsesmæssige styring, administration og forvaltning af Digital Post.

De udførte tilsynshandlinger omhandler dokumentation for Digitaliseringsstyrelsens etablering og opdatering af politikker samt procedurer for kontrol af Digital Post på følgende 3 organisatoriske forretningsområder:

1) Ledelsesstyring med informations- og persondatasikkerhed; fx overordnede politikker, retningslinjer og procedurer i organisationen
2) Kontor med ansvar for vedligeholdelse, udvikling og forvaltning af Digital Post
3) Leverandørstyring i henhold til it-kontraktkrav og underdatabehandleraftale om Digital Post med underleverandør

Som eksempel har tilsynet testet, at der foreligger dokumentation for tavshedserklæring ved ansættelse af medarbejdere i Digitaliseringsstyrelsen samt supplerende sikkerhedsgodkendelse af medarbejdere, der varetager privilegerede opgaver med Digital Post. Tillige har tilsynet testet, at relevante krav til tavshedserklæring af medarbejdere hos underleverandør fremgår af it-kontrakten, og der kan fremlægges revisionserklæringer for leverandørens opfyldelse af krav.

Digital Post 2023 kontrolkatalog med tilsynets udførte test og resultater for perioden 2022

§ 4 Databehandleren handler efter instruks

Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolmål	Udført test	Testresultat
1.1	**§ 4 Databehandleren handler** Stk. 1. og stk 3. Digitaliseringsstyrelsen handler efter instruks fra den dataansvarlige offentlige afsender / juridiske enhed. Digitaliseringsstyrelsen instrueres som databehandler i at sende meddelelser for offentlige afsendere / juridiske enheder til de af de offentlige afsendere / juridiske enheder anførte modtageres digitale postkasser. Denne bestemmelse udgør den databeskyttelsesretlige instruks i henhold til stk. 1.	A) Der foreligger skriftlige procedurer, som indeholder krav om, at Digitaliseringsstyrelsen alene må foretage behandling af personoplysninger, når der foreligger en instruks. B) Der foretages løbende – og mindst en gang årligt – en vurdering af, om procedurerne skal opdateres. C) Digitaliseringsstyrelsen udfører alene den behandling af personoplysninger, som fremgår af instruksen fra den dataansvarlige.	Ad A) Noteret, at der foreligger formaliserede procedurer internt i Digitaliseringsstyrelsen og ved forelæggelse af revisionserklæringer fra underleverandør, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Ad B) Inspiceret, at Digitaliseringsstyrelsens og underleverandørens procedurer indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Ad B) Konstateret, at procedurer er opdateret internt i Digitaliseringsstyrelsen og hos underleverandør. Ad C) Konstateret, at Digitaliseringsstyrelsens ledelse sikrer, at behandling af personoplysninger alene foregår i henhold til instruks, og at dette omfatter underleverandør. Ad C) Inspiceret, ved gennemsyn af dokumentation internt i Digitaliseringsstyrelsen og ved forelæggelse af revisionserklæringer fra underleverandør, at behandlinger af personoplysninger foregår i overensstemmelse med instruksen.	Ingen afvigelser konstateret

Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolmål	Udført test	Testresultat
1.2	**§ 4 Databehandleren handler efter instruks** Stk. 1. og stk. 2. Den dataansvarlige offentlige afsender/juridiske enhed kan give supplerende instruks, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk. Databehandleren underretter omgående den dataansvarlige offentlige afsender / juridiske enhed, hvis en instruks efter vedkommendes mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	A) Der foreligger skriftlige procedurer, som indeholder krav om, at Digitaliseringsstyrelsen skal identificere, opbevare og overholde en eventuel supplerende instruks. B) Der foreligger procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. C) Digitaliseringsstyrelsen foretager løbende – og mindst en gang årligt – en vurdering af, om procedurerne skal opdateres. D) Digitaliseringsstyrelsen overholder den supplerende instruks vedrørende behandling af personoplysninger.	Ad A-B) Noteret, at der foreligger formaliserede procedurer, der sikrer, at Digitaliseringsstyrelsen identificerer, opbevarer og overholder en eventuel supplerende instruks. Ad B) Noteret, at 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. Ad C) Inspiceret, at Digitaliseringsstyrelsens og underleverandørens procedurer indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Ad C) Konstateret, at procedurer er opdateret internt i Digitaliseringsstyrelsen og hos underleverandør. Ad D) Inspiceret, at Digitaliseringsstyrelsen kan fremvise en ajourført liste over de dataansvarlige, der har afgivet supplerende instruks samt de respektive instrukser. Ad D) Forespurgt om ledelsen sikrer, at behandling af personoplysninger foregår i henhold til den eventuelle supplerende instruks. Ad D) Forespurgt om behandlinger af personoplysninger foregår i overensstemmelse med den supplerende instruks.	Det er oplyst, at der ikke er udformet supplerende instrukser til bekendtgørelser. Ingen yderligere afvigelser konstateret.

Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolmål	Udført test	Testresultat
1.3	**§ 4 Databehandleren handler efter instruks** 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.	A) Databehandlerens behandling og opbevaring af personoplysninger skal ske i Danmark. B) Der er etableret en procedure og retningslinjer for behandling samt opbevaring af data i Danmark. C) Der foreligger underskrevede kontraktuelle aftaler om lokationskrav.	Ad A) Noteret, at Digitaliseringsstyrelsen har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af, at behandlingen foregår i Danmark. Ad B) Konstateret, om der foreligger en procedure og retningslinjer for behandling og opbevaring af data på lokationer i Danmark. Ad C) Konstateret, at der fremgår godkendte leverandører i databehandleraftalen mellem Digitaliseringsstyrelsen og underleverandør. Ad C) Undersøgt, at der foreligger underskrevede kontraktuelle aftaler mellem Digitaliseringsstyrelsen og underleverandør om lokationsgaranti. Ad C) Undersøgt ved gennemsyn, at der forefindes dokumentation for aftaler, procedurer og retningslinjer med underleverandør, at opbevaring af personoplysninger alene foretages på lokaliteter i Danmark.	Ingen afvigelser konstateret.

§ 5 Fortrolighed

Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolmål	Udført test	Testresultat
2.1	**§ 5 Fortrolighed** Stk. 1. Digitaliseringsstyrelsen skal som databehandler sikre, at de personer, der er autoriseret til at behandle personoplysninger på vegne af offentlige afsendere / juridiske enheder, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.	A) Det foreligger procedure for indgåelse og dokumentation af tavsheds- og fortrolighedsaftale med medarbejdere. B) Der foreligger procedure og dokumentation for tavshedspligt.	Ad A) Konstateret, at der er indgået tavsheds- og fortrolighedsaftale med medarbejdere internt i Digitaliseringsstyrelsen. Ad A) Undersøgt, at underleverandør er forpligtet til skriftlig tavsheds- og fortrolighedsaftale med medarbejdere. Ad B) Konstateret, at der er etableret procedurer for tavsheds- og fortrolighedsaftale med medarbejdere internt i Digitaliseringsstyrelsen og hos underleverandør. Ad B) Noteret ved gennemsyn af revisionserklæringer fra underleverandør, at der foreligger dokumentation for tavsheds- og fortrolighedsaftale.	Ingen afvigelser konstateret.

§ 6 Behandlingssikkerhed

Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolmål	Udført test	Testresultat
2.2	**§ 6 Behandlingssikkerhed** Stk. 2. nr. 1-4 og stk. 3. nr. 1-2. Digitaliseringsstyrelsen iværksætter alle foranstaltninger, der kræves i henhold til databeskyttelsesforordningens artikel 32 om behandlingssikkerhed på baggrund af en risikovurdering. Digitaliseringsstyrelsen stiller på sin hjemmeside en sammenfatning af den foretagne risikovurdering til rådighed for de dataansvarlige offentlige afsendere / juridiske enheder, så risikovurderingen kan indgå i de dataansvarliges egne risikovurderinger. 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. 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.	A) Der foreligger dokumentation for en risikovurdering, som er stillet til rådighed for de dataansvarlige. B) Der er fastlagt og implementeret passende interne foranstaltninger i eget informationssikkerhedsledelsessystem. C) Der foreligger procedurer for årlig afprøvning, vurdering og evaluering. D) Der gives den fornødne instruktion til egne medarbejdere, som behandler personoplysninger.	Ad A) Noteret, at der foreligger dokumentation for en ledelsesgodkendt risikovurdering af Digital Post og der er implementeret foranstaltninger. Ad A) Modtaget dokumentation for, at Digital Post er et samfundskritisk infrastruktursystem i Danmark, og Digitaliseringsstyrelsen har besluttet at offentliggøre et selvstændigt notat om risici til de dataansvarlige, som tager afsæt i resultater fra risikovurderingen og konsekvensanalysen af Digital Post. Ad A) Modtaget dokumentation for, at underleverandør har foretaget en risikovurdering og implementeret de tekniske foranstaltninger. Ad B) Konstateret, at der er etableret et udvalg for informationssikkerhedsledelse og implementeret politikker, procedurer og retningslinjer i Digitaliseringsstyrelsen og hos underleverandør. Ad C) Noteret, at der foreligger procedurer for årlig afprøvning, vurdering og evaluering i Digitaliseringsstyrelsen og hos underleverandør. Ad D) Noteret, at der gives instruktion om behandling af personoplysninger til medarbejdere i Digitaliseringsstyrelsen og hos underleverandør.	Det er oplyst, at der udestår mindre justeringer af materiale om informationssikkerhed ifm. etablering af Digitaliseringsstyrelsen under nyt ministerområde. Ingen yderligere afvigelser konstateret.

Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolmål	Udført test	Testresultat
2.3	**§ 6 Behandlingssikkerhed** Stk. 3. nr. 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.	A) Digitaliseringsstyrelsen sikrer, at der foreligger skriftlige procedurer, som indeholder krav om, at Digitaliseringsstyrelsen instruerer sine medarbejdere om relevante databeskyttelsespolitikker og -procedurer, og hvordan instruktionen skal foregå. B) Der foreligger skriftlige procedurer, som indeholder krav om, at Digitaliseringsstyrelsen uddanner sine medarbejdere i relevante databeskyttelsespolitikker og -procedurer, og hvordan uddannelsen skal foregå, herunder ved relevante awarenssaktiviteter, interne oplæg, workshops etc. C) Digitaliseringsstyrelsen sikrer, at der foreligger skriftlige procedurer, som indeholder krav og muliggør, at leverandøren har de nødvendige uddannelses- og awarenessaktiviteter og løbende uddanner medarbejdere i sikker behandling af personoplysninger i overensstemmelse med de nævnte regler og procedurer. D) Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Ad A) Noteret, at der findes krav og procedurer for hvordan Digitaliseringsstyrelsen instruerer sine medarbejdere om relevante politikker og procedurer om persondatasikkerhed. Ad B) Noteret, at Digitaliseringsstyrelsen årligt og regelmæssigt uddanner og træner sine medarbejdere i persondatasikkerhed, herunder ved relevante awarenssaktiviteter, interne oplæg, workshops etc. Ad B) Noteret, at Digitaliseringsstyrelsen har en opdateret statistik over, hvor mange medarbejdere har deltaget i relevant træning omkring informations- og persondatasikkerhed. Ad C) Noteret, at Digitaliseringsstyrelsen har stillet kontraktkrav til underleverandøren om årlig og regelmæssig awarenesstræning relateret til persondatasikkerhed, herunder at der foreligger revisionserklæringer fra leverandøren om efterlevelse heraf. D) Noteret, at der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Ingen afvigelser konstateret.

§ 7 Autorisation og adgangskontrol

Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolmål	Udført test	Testresultat
2.4	**§ 7 Autorisation og adgangskontrol** 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.	A) Der er etableret proces for oprettelse og nedlæggelse af brugere. B) Der skal foreligge procedurer for autorisation og adgangskontrol. C) Der skal være etableret proces for styring og kontrol med privilegerede rettigheder. D) Der skal fastlægges opfølgende kontrol med autorisation, adgang og rettigheder. E) Der skal mindst én gang årligt gennemføres kontrol med autorisation, adgang og rettigheder.	Ad A) Forespurgt om der er etableret proces for oprettelse og nedlæggelse af brugere i Digitaliseringsstyrelsen og hos underleverandør. Ad B) Noteret, at der er procedurer for autorisation og løbende adgangskontrol i Digitaliseringsstyrelsen og hos underleverandør, som bliver ledelsesgodkendt. Ad C) Noteret, at der er proces for styring og kontrol med privilegerede rettigheder i Digitaliseringsstyrelsen og hos underleverandør, som ledelsesgodkendes. Ad D) Noteret, at der er fastlagt faste perioder for kontroller med autorisation, adgang og rettigheder i Digitaliseringsstyrelsen og hos underleverandør. Ad E) Konstateret, at der er dokumentation for gennemførte kontroller med autorisation, adgang og rettigheder, herunder at dette sker mindst én gang årligt i Digitaliseringsstyrelsen og hos underleverandør.	Ingen afvigelser konstateret.

§ 8 Anvendelse af underdatabehandlere

Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolmål	Udført test	Testresultat
3.1	**§ 8 Anvendelse af underdatabehandlere** Stk. 1., stk. 2. og stk. 3. 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). 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. 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.	A) Der skal foreligge procedurer for indgåelse af gyldige underdatabehandleraftale mellem Digitaliseringsstyrelsen og underdatabehandlere. B) Der skal foreligge procedurer, som sikrer, at underdatabehandleren kan stille de fornødne garantier for, at de gennemfører passende tekniske og organisatoriske sikkerhedsforanstaltninger. C) Der skal foreligge en gyldig underdatabehandleraftale mellem Digitaliseringsstyrelsen og underdatabehandler. D) Der foreligger information om underdatabehandlere på Digitaliseringsstyrelsens hjemmeside.	Ad A) Noteret, at der er etableret interne processer, som sikrer gyldig underskrevet underdatabehandeleraftaler mellem Digitaliseringsstyrelsen og underleverandører. Ad B) Konstateret, at der er indgået kontrakt og databehandleraftale, som sikrer de fornødne garantier for, at underleverandøren gennemfører passende tekniske og organisatoriske sikkerhedsforanstaltninger. Ad B) Konstateret, er der foreligger årlig revisionserklæringer fra underleverandøren, som dokumenterer aftalte krav til de tekniske og organisatoriske sikkerhedsforanstaltninger. Ad C) Noteret, at der er indgået en gyldig underskrevet underdatabehandeleraftale mellem Digitaliseringsstyrelsen og underleverandør. Ad D) Observeret, at Digitaliseringsstyrelsen har offentliggjort informationer om underdatabehandlere på hjemmeside.	Ingen afvigelser konstateret.

Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolmål	Udført test	Testresultat
3.2	**§ 8 Anvendelse af underdatabehandlere** Stk. 4. og stk. 5. Digitaliseringsstyrelsen sørger for at pålægge underdatabehandlere de samme databeskyttelsesforpligtelser, som dem, der er fastsat ved denne	A) Det skal sikres, at kontrakter og aftaler med tredjepartsleverandører er juridisk bindende og leverandørerne pålægges at overholde Europæisk og dansk lovgivning herunder bl.a. supplerende databeskyttelsesregler og bekendtgørelser.	Ad A) Noteret, at Digitaliseringsstyrelsen har etableret processer som sikrer, at kontrakter og aftaler med tredjepartsleverandører er juridisk bindende og leverandørerne pålægges at overholde europæisk og dansk lovgivning. Ad A) Konstateret, at der er indgået juridisk bindende kontrakt og aftale mellem Digitaliseringsstyrelsen og underleverandøren, som	Ingen afvigelser konstateret.

	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. 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.	B) Leverandøren skal som kontraktansvarlig, forinden brug af en underleverandør, indgå en skriftlig aftale med denne underleverandør, hvori underleverandøren som minimum pålægges de samme forpligtelser, som leverandøren har påtaget sig ved Databehandleraftalen.	til enhver tid forpligter leverandøren til at overholde gældende europæisk og dansk lovgivning. Ad B) Noteret, at Digitaliseringsstyrelsen har stillet krav og vilkår til underleverandøren om indgåelse af underdatabehandleraftale ved behandling af personoplysninger hos underleverandørens leverandør. Ad B) Noteret, at der foreligger revisionserklæringer fra underleverandøren vedrørende kontrol med underleverandørens databehandleraftaler med deres leverandører.	

Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolmål	Udført test	Testresultat
3.3	**§ 8 Anvendelse af underdatabehandlere** Stk. 6. nr. 1. 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 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 / juridiske enheder.	A) Der foreligger procedurer, som sikrer, at der foretages tilsyn med underdatabehandlerens overholdelse af underdatabehandleraftalen. B) Der stilles krav til levering af årlige revisionserklæringer fra tredjepartsleverandører, som er udarbejdet af uafhængige revisorer. C) Der stilles krav til, at underleverandøren for Digital Post årligt afgiver revisionserklæringer for opfyldelse af forpligtelser i kontrakt og underdatabehandleraftale. D) Revisionserklæringer fra underleverandør stilles til rådighed for de dataansvarlige.	Ad A) Verificeret, at Digitaliseringsstyrelsen har etableret model og proces for årlig leverandørtilsyn med overholdelse af underdatabehandleraftaler. Ad A) Verificeret, at der foreligger ledelsesgodkendt dokumentation for gennemført leverandørtilsyn med overholdelse af underdatabehandleraftaler. Ad B) Noteret, at Digitaliseringsstyrelsen stiller krav til tredjepartsleverandører vedr. levering af årlige revisionserklæringer, som er udarbejdet af uafhængige statsautoriserede revisorer. Ad C) Konstateret, at Digitaliseringsstyrelsen har stillet krav i kontrakt og underdatabehandleraftale med underleverandøren for Digital Post årligt afgiver revisionserklæringer for opfyldelse af forpligtelser om informationssikkerhed og persondatasikkerhed. Ad D) Observeret, at Digitaliseringsstyrelsen har stillet de årlige revisionserklæringer fra underleverandør til rådighed for de dataansvarlige.	Ingen afvigelser konstateret.

§ 9 Overførsel til tredjelande eller internationale organisationer

Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolmål	Udført test	Testresultat
4.1	**§ 9 Overførsel til tredjelande eller internationale organisationer** Stk. 1., stk. 2., stk. 3. og stk. 4. Digitaliseringsstyrelsen vil som databehandler for Digital Post ikke overføre personoplysninger til tredjelande eller internationale organisationer, jf. § 4, stk. 8. 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 / juridiske enhed og skal altid ske i overensstemmelse med	A) Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren kun overfører personoplysninger til tredjelande efter aftalen med den dataansvarlige og gyldigt overførselsgrundlag. A) Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. B) Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige. B) Databehandleren skal kunne dokumentere, hvornår databehandleren har overført personoplysninger til tredjelande, herunder hvilke oplysninger	Ad A) Inspiceret, at der er indført procedurer, der sikrer, at personoplysninger kun overføres til tredjelande efter aftale med den dataansvarlige og på baggrund af et gyldigt overførselsgrundlag. Ad A) Noteret, at procedurerne løbende og årligt opdateres. Ad B) Noteret, at Digitaliseringsstyrelsen har en oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer. Ad B) Verificeret, at der er dokumentation for, at Digitaliseringsstyrelsens overførsler sker efter aftale, godkendelse og instruks fra den dataansvarlige. Ad C) Noteret at der foreligger procedurer og dokumentation for et gyldigt overførselsgrundlag af personoplysninger, og at overførsler kun sker i det omfang, det er aftalt med den dataansvarlige.	Ingen afvigelser konstateret.

	databeskyttelsesforordningens kapitel V og retshåndhævelseslovens afsnit VII (fsva. offentlige afsendere). Uden dokumenteret instruks fra den dataansvarlige offentlige afsender / juridiske enhed 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. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som Digitaliseringsstyrelsen ikke er blevet instrueret i at foretage af den dataansvarlige offentlige afsender / juridiske enhed, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Digitaliseringsstyrelsen er underlagt, skal Digitaliseringsstyrelsen underrette den dataansvarlige offentlige afsender / juridiske enhed om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser. Ved overførsler omfattet af stk. 2, er den offentlige afsender / juridiske enhed ansvarlig for at sikre, at der foreligger et gyldigt overførselsgrundlag i henhold til databeskyttelsesforordningens kapitel V og retshåndhævelseslovens afsnit VII, kapitel 17 (fsva. offentlige afsendere).	der er overført til hvilke tredjelande og hvornår. C) Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.		

§ 10 Bistand til den dataansvarlige

Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolmål	Udført test	Testresultat
5.1	**§ 10 Bistand til den dataansvarlige** Stk. 1. og stk. 2. nr. 1-2. (Oplysningspligt) Digitaliseringsstyrelsen skal i medfør af stk. 1, så vidt muligt bistå den offentlige afsender / juridiske enhed i forbindelse med, at den offentlige afsender / juridiske enhed 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.	A) Digitaliseringsstyrelsen sikrer, at der foreligger skriftlige procedurer, som indeholder krav om og beskriver, hvordan databehandleren rettidigt skal bistå den dataansvarlige med at sikre overholdelse af oplysningspligten. B) Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Ad A) Inspiceret Digitaliseringsstyrelsens procedurer vedrørende bistand til de dataansvarlige, herunder offentliggørelse af informationer på hjemmeside om Digital Post, som sikrer overholdelse af oplysningspligten. Ad A) Noteret, at der er etableret procedurer hos underleverandør vedrørende, hvordan der ydes rettidig bistand til overholdelse af oplysningspligten til den dataansvarlige i relation til de registreredes rettigheder. Ad B) Noteret, at der foretages løbende - og mindst én gang årligt - vurdering af, om procedurerne skal opdateres.	Ingen afvigelser konstateret.

Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolmål	Udført test	Testresultat
5.2	**§ 10 Bistand til den dataansvarlige** Stk. 1. og stk. 2. nr. 3-8. (De registreredes rettigheder) Digitaliseringsstyrelsen skal i medfør af stk. 1, så vidt muligt bistå den offentlige afsender / juridiske enhed i forbindelse med, at den offentlige afsender / juridiske enhed i dens rolle som	A) Digitaliseringsstyrelsen sikrer, at der foreligger skriftlige procedurer, som indeholder krav om og muliggør, at databehandleren rettidigt skal bistå den dataansvarlige i relation til de registreredes rettigheder. A) Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Ad A) Inspiceret Digitaliseringsstyrelsens procedurer vedrørende bistand til de dataansvarlige, herunder offentliggørelse af informationer på hjemmeside om Digital Post og hvordan bistand skal foregå Ad A) Noteret, at der foretages løbende - og mindst én gang årligt - vurdering af, om procedurerne skal opdateres.	Ingen afvigelser konstateret.

	dataansvarlig skal sikre overholdelsen af nedenstående regler i databeskyttelsesforordningen og retshåndhævelsesloven: 3) Den registreredes indsigtsret, jf. databeskyttelsesforordningens artikel 15 og retshåndhævelseslovens § 15 (fsva. offentlige afsendere). 4) Retten til berigtigelse, jf. databeskyttelsesforordningens artikel 16 og retshåndhævelseslovens § 17, stk. 1 (fsva. offentlige afsendere). 5) Retten til sletning (»retten til at blive glemt«), jf. databeskyttelsesforordningens artikel 17 og retshåndhævelseslovens § 17, stk. 2 (fsva. offentlige afsendere). 6) Retten til begrænsning af behandling, jf. databeskyttelsesforordningens artikel 18 og retshåndhævelseslovens § 17, stk. 3 (fsva. offentlige afsendere). 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.	B) Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Ad B) Inspiceret, at der foreliggende procedurer for bistand til den dataansvarlige, og det er defineret, hvordan bistand skal finde sted til de registrerede i forbindelse med: Udlevering, rettelser, sletning, begrænsning af oplysninger, underretningspligt og retten til indsigelser. Ad B) Noteret, at der findes diagram med dataflow og dokumentation for it-systemer hos underleverandør understøtter procedurer for bistand til de registrerede.	

Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolmål	Udført test	Testresultat
5.3	**§ 10 Bistand til den dataansvarlige** Stk. 3. nr. 1. (Behandlingssikkerhed) Digitaliseringsstyrelsen skal under hensyntagen til behandlingens karakter bistå den enkelte offentlige afsender / juridiske enhed 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.	A) Der foreligger procedurer, som sikrer bistand til de dataansvarlige med at vurdere og etablere passende sikkerhedsforanstaltninger i forhold til de identificerede risici. B) Der foretages løbende – og mindst en gang årligt – en vurdering om risici skal opdateres.	Ad A) Noteret, at Digitaliseringsstyrelsen har etableret procedurer og materiale, som sikrer bistand til de dataansvarlige med at vurdere mulige sikkerhedsforanstaltninger. Ad B) Inspiceret, at Digitaliseringsstyrelsen løbende – og mindst en gang årligt – opdaterer risikobilledet og foranstaltninger på baggrund af en fornyet risiko- og trusselsvurdering.	Ingen afvigelser konstateret.

Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolmål	Udført test	Testresultat
5.4	**§ 10 Bistand til den dataansvarlige** Stk. 3. nr. 2. (Anmeldelse af brud på persondatasikkerheden) Digitaliseringsstyrelsen skal under hensyntagen til behandlingens karakter bistå den enkelte offentlige afsender / juridiske enhed i forbindelse med, at denne skal sikre overholdelsen af: 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.	A) Der foreligger skriftlige procedurer, som sikrer, at databehandleren rettidigt kan bistå den dataansvarlige i relation til at anmelde brud på persondatasikkerheden til Datatilsynet inden for 72 timer. B) Der foreligger krav og procedurer, der sikrer, at databehandleren kan yde bistand til den dataansvarlige ved anmeldelse til Datatilsynet, herunder karakteren og sandsynlige konsekvenser af bruddet på persondatasikkerheden samt mulige foranstaltninger til håndtering af bruddet. C) Der foreligger et skriftligt overblik vedrørende opfølgning og status på årets relevante databeskyttelsesmæssige hændelser, underretninger og anmeldelser til Datatilsynet. D) Der skal foretages løbende – og mindst en gang årligt – vurdering af, om procedurer skal opdateres.	Ad A) Konstateret, at Digitaliseringsstyrelsen har etableret procedurer og retningslinjer, som sikrer rettidig bistand til de dataansvarlige ved håndtering af sikkerhedshændelser for Digital Post, herunder evt. underretningsbrev til de dataansvarlige om karakteren af bruddet, konsekvenser og foranstaltninger til håndtering af bruddet samt anmeldelse til Datatilsynet. Ad B) Konstateret, at 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. Ad C) Konstateret at der er dokumentation for registrerede databeskyttelsesmæssige hændelser, herunder opfølgning, underretning, status og evt. anmeldelser til Datatilsynet. Ad C) Konstateret, at Digitaliseringsstyrelsen har anmeldt 10 brud på persondatasikkerheden til Datatilsynet i 2022 og relevante borgere, myndigheder og virksomheder samtidigt er underrettet om hændelserne. Hertil er noteret, at ikke alle hændelser er anmeldt inden for tidsfristen på 72 timer og Datatilsynet har afsluttet 7 anmeldelser uden grundlag for yderligere handlinger.	Det er oplyst, at der fortsat udestår tilbagemelding fra Datatilsynet på 3 anmeldte hændelser. Ingen afvigelser konstateret.

			Ad D) Noteret, at Digitaliseringsstyrelsen løbende – og mindst en gang årligt – opdaterer procedurer og retningslinjer vedrørende håndtering af sikkerhedshændelser.	
Nr.	**Forpligtelser jf. bekendtgørelserne**	**Kontrolmål**	**Udført test**	**Testresultat**
5.5	**§ 10 Bistand til den dataansvarlige** Stk. 3. nr. 3. (Underretning om brud på persondatasikkerheden) Digitaliseringsstyrelsen skal under hensyntagen til behandlingens karakter bistå den enkelte offentlige afsender / juridiske enhed i forbindelse med, at denne skal sikre overholdelsen af: 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.	A) Der foreligger skriftlige procedurer, som sikre, at databehandleren rettidigt underretter den dataansvarlige ved anmeldelse af brud på persondatasikkerheden til Datatilsynet. B) Der foreligger krav og procedurer, der sikre at databehandleren underretter de dataansvarlige ved brud på persondatasikkerheden. Ad C: Der skal foretages løbende – og mindst en gang årligt – vurdering og opdatering af procedurer vedr. underretning.	Ad A) Konstateret, at Digitaliseringsstyrelsen har etableret procedurer og retningslinjer for behandling af brud på persondatasikkerheden, som sikre at de dataansvarlige rettidig bliver underrettet, når et brud sandsynligvis vil indebære en høj risiko for de registreredes rettigheder. Ad B) Konstateret, at 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. Ad C) Noteret, at Digitaliseringsstyrelsen løbende – og mindst en gang årligt – opdaterer procedurer og retningslinjer vedrørende håndtering af underretning om brud på persondatasikkerheden.	Ingen afvigelser konstateret.
Nr.	**Forpligtelser jf. bekendtgørelserne**	**Kontrolmål**	**Udført test**	**Testresultat**
5.6	**§ 10 Bistand til den dataansvarlige** Stk. 3. nr. 4. (Gennemførelse af konsekvensanalyse) Digitaliseringsstyrelsen skal under hensyntagen til behandlingens karakter bistå den enkelte offentlige afsender / juridiske enhed i forbindelse med, at denne skal sikre overholdelsen af: 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.	A) Der foreligger skriftlige krav og procedurer, som beskriver, hvordan databehandleren rettidigt bistår den dataansvarlige med at overholde forpligtelser til at gennemføre en konsekvensanalyse vedrørende databeskyttelse. B) Der er udarbejdet en konsekvensanalyse, som er sendt i høring hos Datatilsynet hvis det indebære en høj risiko for de registreredes rettigheder. C) Der foretages løbende – og mindst en gang årligt – vurdering af konsekvensanalysen om databeskyttelse skal opdateres. C) Der foretages løbende – og mindst en gang årligt – vurdering af relevant materiale til de dataansvarlig skal opdateres og offentliggøres.	Ad A) Noteret, at Digitaliseringsstyrelsen har etableret procedurer, som sikrer rettidig bistand til den dataansvarlige med at overholde forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse. Ad B) Konstateret, at Digitaliseringsstyrelsen har udformet ledelsesgodkendt konsekvensanalyse, der viser, at risici er nedbragt til *mellem* og dermed ikke skal sendes i høring hos Datatilsynet, eftersom behandlingen ikke vil føre til høj risiko for de registrerede jf. databeskyttelsesforordningens artikel 36, stk. 1. Ad A) Noteret, at Digitaliseringsstyrelsen på baggrund af konsekvensanalysen har identificerede risici forbundet med rollen som databehandler og har udformet et selvstændigt notat indeholdende beskrivelse af håndtering og begrænsning af risici samt en række forslag til eventuelle yderligere foranstaltninger hos de dataansvarlige. Ad B) Noteret, at Digitaliseringsstyrelsen har offentliggjort selvstændigt notat, som bistand til de dataansvarliges arbejde med egen konsekvensanalyse samt valg af foranstaltninger til begrænsning af risici, såfremt det vurderes nødvendigt. Ad C) Noteret, at Digitaliseringsstyrelsen løbende – og mindst en gang årligt – vurderer om konsekvensanalysen vedrørende databeskyttelse skal opdateres, herunder om der skal indhentes supplerende oplysninger fra underleverandøren. Ad C) Noteret, at Digitaliseringsstyrelsen løbende – og mindst en gang årligt – på baggrund af konsekvensanalysen vurderer, om notat om risici til de dataansvarlige skal opdateres og offentliggøres på hjemmesiden.	Ingen afvigelser konstateret.
		§ 11 Underretning om brud på persondatasikkerheden til Datatilsynet		
Nr.	**Forpligtelser jf. bekendtgørelserne**	**Kontrolmål**	**Udført test**	**Testresultat**
6.1	**§ 11 Underretning om brud på persondatasikkerhed til Datatilsynet** Stk. 2. og stk. 4. nr. 1-3. Digitaliseringsstyrelsens underretning til den dataansvarlige offentlige afsender / juridiske enhed 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. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som i medfør af	A) Der foreligger krav og procedurer, som sikrer, at databehandleren overholder sin forpligtelse om rettidig underretning til de dataansvarlige senest 48 timer efter, der er konstateret brud på persondatasikkerheden med evt. henblik på anmeldelse til Datatilsynet inden for 72 timer. B) Der foreligger krav og procedurer, der sikrer at databehandleren underretter de dataansvarlige om karakteren af bruddet, konsekvenser og mulige foranstaltninger til håndtering af bruddet. C) Der skal foretages løbende – og mindst en gang årligt – vurdering og opdatering af procedurer vedr. underretning.	Ad A) Konstateret, at Digitaliseringsstyrelsen har etableret procedurer og retningslinjer for behandling af brud på persondatasikkerheden, som sikrer, at de dataansvarlige rettidig bliver underrettet, når der er konstateret sandsynlighed for brud på persondatasikkerheden. Ad B) Konstateret, at 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. Ad C) Noteret, at Digitaliseringsstyrelsen løbende – og mindst en gang årligt – opdaterer procedurer og retningslinjer vedrørende håndtering af brud på persondatasikkerheden.	Ingen afvigelser konstateret.

	databeskyttelsesforordningens artikel 33, stk. 3 og retshåndhævelseslovens § 28, stk. 3, skal fremgå af den dataansvarlige offentlige afsenders / juridiske enheds anmeldelse af bruddet til Datatilsynet: 1) Karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne … 2) De sandsynlige konsekvenser af bruddet på persondatasikkerheden. 3) De foranstaltninger, som Digitaliseringsstyrelsen har udført …			

§ 12 Sletning af personoplysninger (For offentlige afsendere og juridiske enheder)

Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolmål	Udført test	Testresultat
7.1	**§ 12 Sletning af personoplysninger** For offentlige afsendere: 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. **§ 12 Sletning af personoplysninger** For juridiske enheder: Digitaliseringsstyrelsens databehandling i medfør af denne bekendtgørelse ophører: 1) Ved transmission 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. Digitaliseringsstyrelsen sletter ikke de i § 3 nævnte personoplysninger, da meddelelserne efter levering er overgået til modtagernes råde- og ejendomsret. 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.	A) Digitaliseringsstyrelsen sikrer, at der foreligger skriftlige procedurer, som indeholder krav om, at der foretages 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. B) Der foretages løbende - og mindst en gang årligt - vurdering af, om procedurerne skal opdateres. C) Digitaliseringsstyrelsen opbevarer ikke personoplysninger på vegne af de dataansvarlige juridiske enheder på tidspunktet efter, at de juridiske enheder har valgt at slette deres meddelelser i deres digitale postkasse. D) Der foreligger skriftlige procedurer, som indeholder krav om - og beskriver processen herfor - at Digitaliseringsstyrelsen sikrer, at midlertidige filer, der indeholder personoplysninger, slettes eller anonymiseres, f.eks. i test- og udviklingsmiljøer. E) Der foretages løbende - og mindst en gang årligt - vurdering af, om procedurerne skal opdateres. F) Der foreligger skriftlige procedurer, som fastlægger ansvaret for og beskriver behandling og sikker destruktion af ind- og uddatamateriale samt anvendelse af edb-udstyr. Procedurerne skal indeholde retningslinjer, der understøtter, at der ved tilintetgørelse af uddatamateriale træffes de fornødne sikkerhedsforanstaltninger mod, at materialet misbruges eller kommer til uvedkommendes kendskab. Procedurerne skal også indeholder retningslinjer, der understøtter, at der i forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier træffes de fornødne sikkerhedsforanstaltninger mod, at uvedkommende får adgang til personoplysningerne. G) Der foretages løbende - og mindst en gang årligt - vurdering af, om procedurerne skal opdateres.	Ad A) Noteret, at 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. Ad B) Noteret, at procedurerne om opbevaring og sletning vurderes og opdateres en gang om året. Ad C) Noteret, at ved ophør af databehandlinger, at der er indhentet revisionserklæringer for at underleverandøren af Digital Post overholder specifikke krav til opbevaringsperiode og sletterutiner, så Digitaliseringsstyrelsen ikke opbevarer personoplysninger efter tidspunktet for, hvornår modtageren har slettet meddelelsen fra sin digital postkasse. Ad D) Noteret, at der foreligger skriftlige krav og procedurer, så Digitaliseringsstyrelsen sikrer, at midlertidige filer, der indeholder personoplysninger, slettes eller anonymiseres, f.eks. i test- og udviklingsmiljøer. Ad E) Noteret, at procedurerne for sletning af midlertidige filer vurderes og opdateres en gang om året. Ad F) Inspiceret, at der foreligger skriftlige procedurer, som fastlægger ansvaret for og beskriver behandling og sikker destruktion af ind- og uddatamateriale samt anvendelse af edb-udstyr. Ad G) Noteret, at procedurerne for destruktion af ind- og uddatamateriale samt anvendelse af edb-udstyr vurderes og opdateres en gang om året.	Ingen afvigelser konstateret.

digst.dk