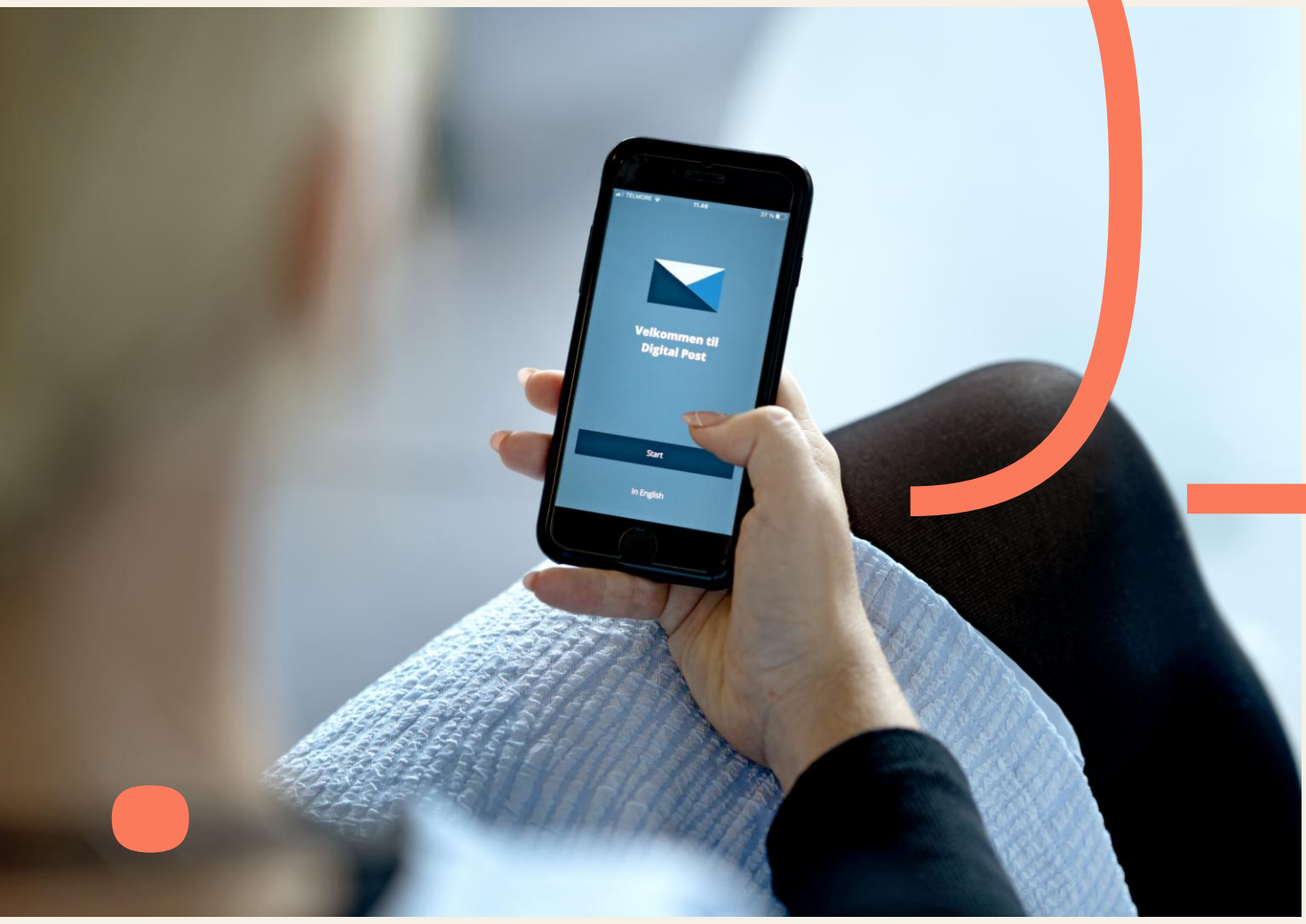
Digitaliserings-
styrelsen

Digital Post

Redegørelse om tilsyn med behandling af personoplysninger i 2023



september 2024

Indhold

Udtalelse, konklusion og oplysningspligt

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

Ledelsens udtalelse
Den sammenfattende konklusion for perioden 2023 er udformet på grundlag af de forhold, der er beskrevet i denne redegørelse om Digital Post til de dataansvarlige offentlige afsendere og juridiske enheder (herefter virksomheder).

Ledelsen bekræfter, at 2024-redegørelsen er udfærdiget af Digitaliseringsstyrelsen og retvisende beskriver konklusionen for det gennemførte tilsyn med behandling af personoplysninger i Digital Post for perioden 2023.

Konklusion
Det vurderes, at Digitaliseringsstyrelsen som systemansvarlig for Digital Post har overholdt de databeskyttelsesretlige regler for behandling af personoplysninger.

Konklusionen bygger på tilsynets samlede indtryk fra Digitaliseringsstyrelsens opfyldelse af forpligtelser fordelt på 68 kontrolmål. De udvalgte kontroller er baseret på regler i EU's databeskyttelsesforordning[1], den danske databeskyttelseslov[2] og bekendtgørelserne[3] om behandling af personoplysninger i Digital Post.

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

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

For så vidt angår hændelseshåndtering i 2023 har Digitaliseringsstyrelsen registreret fem brud på persondatasikkerheden i Digital Post. Aktuelt udestår der tilbagemelding fra Datatilsynet på de fem anmeldte hændelser.

[1] 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).
[2] 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.

[3] 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.

Om redegørelsen

Digitaliseringsstyrelsen har i 2024 gennemført tilsyn med behandling af personoplysninger i Digital Post for perioden 2023 på vegne af de dataansvarlige offentlige afsendere og virksomheder. Denne redegørelse er udfærdiget af kontor med ansvar for tilsynsopgaver og udgør en skriftlig fremstilling af det udførte tilsyn.

Redegørelsen er udarbejdet ifølge bekendtgørelserne om Digital Post. Hensigten er at stille de nødvendige oplysninger til rådighed for de dataansvarlige for at påvise overholdelse af de databeskyttelsesretlige regler. I redegørelsen beskrives det bagvedliggende tilsynsarbejde med Digital Post og resultatet af de gennemførte kontrolaktiviteter, som fremgår af kontrolkatalog sidst i redegørelsen.

Den årlige redegørelse tilpasses i takt med de dataansvarliges behov for indsigt i de udførte tilsynshandlinger.

Oplysningspligt og kontaktoplysninger

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

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

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

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

Offentliggørels af tilsynsmateriale

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

- Digitaliserings- og Ligestillingsministeriets departements 2024 tilsynsrapport om Digitaliseringsstyrelsens tilsynspligt med behandling af personoplysninger i Digital Post
- Digitaliseringsstyrelsens 2024 redegørelse om tilsyn med behandling af personoplysninger i Digital Post for perioden 2023
- Notat om risici ved Digitaliseringsstyrelsens behandling af personoplysninger som databehandler
- Specifikke revisionserklæringer om Digital Post for perioden 2023 fra Digitaliseringsstyrelsens underleverandør.

Lovgivning, formål og dataansvar

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

Retsgrundlag
Digitaliseringsstyrelsen har ifølge LBK nr. 686 af 15. april 2021 om Digital Post fra offentlige afsendere om Digital Post (herefter Digital Post-loven)[4] systemansvaret for udvikling, drift, vedligehold 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 to 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)[5]. Bekendtgørelserne regulerer det ansvar og de forpligtelser, som Digitaliseringsstyrelsen er underlagt som databehandler for henholdsvis offentlige afsendere og juridiske enheder i forbindelse med forsendelse og opbevaring af postmeddelelser via Digital Post.

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. I forlængelse heraf fremgår det, at Digitaliserings- og Ligestillingsministeriets departement fører et tilsyn med Digitaliseringsstyrelsen på vegne af de dataansvarlige. Departementet udarbejder en årlig tilsynsrapport, der udgør det databeskyttelsesretlige tilsyn, de dataansvarlige kan føre med Digitaliseringsstyrelsen.

Formål med behandling af personoplysninger
Digitaliseringsstyrelsens behandling af personoplysninger i Digital Post finder anvendelse ved tilslutning af offentlige afsendere, fysiske personer og virksomheder til den fællesoffentlige postløsning. Behandlingen af personoplysninger sker med henblik på at muliggøre en sikker digital kommunikation af postmeddelelser og stille digitale postkasser til rådighed for fysiske personer og virksomheder.

Til at understøtte formålet behandler Digitaliseringsstyrelsen personoplysninger i Digital Post, som er nødvendig i forbindelse med drift, vedligeholdog forvaltning af postløsningen.

Dataansvarlig og databehandler
Rollefordelingen som henholdsvis dataansvarlig og databehandler følger af Digital Post-loven § 2 a, stk. 3 og 4:

- Digitaliseringsstyrelsen er dataansvarlig for behandling af personoplysninger i forbindelse

[4] LBK nr. 686 af 15. april 2021 Bekendtgørelse af lov om Digital Post fra offentlige afsendere om Digital Post
[5] 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.

med levering af meddelelser, vedligehold, udvikling og forvaltning af den driftstekniske løsning til Digital Post.
- Offentlige afsendere er dataansvarlige for indholdet af de meddelelser, de sender via Digital Post. Digitaliseringsstyrelsen er databehandler for offentlige afsenderes forsendelse af meddelelser.
- Virksomheder er dataansvarlige for indholdet af de meddelelser, de sender via og opbevarer i Digital Post. Digitaliseringsstyrelsen er databehandler for virksomheders forsendelse og opbevaring af meddelelser.

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

De næste afsnit skitserer rollefordelingen mellem den dataansvarlig og databehandler ved forsendelse, opbevaring og indhold af postmeddelelser i Digital Post. En uddybende beskrivelse for borgere, myndigheder og virksomheder findes på Digitaliseringsstyrelsens hjemmeside.

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 i henhold til de instrukser, som Digitaliseringsstyrelsen modtager fra de offentlige afsendere. Digitaliseringsstyrelsen har således ikke indflydelse på, hvornår postmeddelelser er afsendt eller indholdet af meddelelserne.

Offentlige afsendere har pligt til at oprette et system til modtagelse og opbevaring af postmeddelelser (”modtagesystem”). Oprettelse af et modtagesystem medfører, at Digitaliseringsstyrelsen ikke opbevarer postmeddelelser på de offentlige afsenderes vegne, og som følge heraf er Digitaliseringsstyrelsen ikke databehandler for opbevaringen, jf. § 2 a i Digital Post-loven.

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. i Digital Post-loven.

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

Kategorier af personoplysninger
Digitaliseringsstyrelsen behandler oplysninger om følgende kategorier af registrerede personer:

- Fysiske personer, herunder børn
- Ansatte hos myndigheder
- Ansatte hos virksomheder

I tilknytning hertil indsamler Digitaliseringsstyrelsen personoplysninger fra blandt andet CVR-registret og Statstidende og behandler personoplysninger såsom personnumre, CVR-numre, e-mail og telefonnumre eller lignende, jf. § 2 a i Digital Post-loven. Indsamling og behandling af nedenstående 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 identifikationsnr.)
- CVR-nummer (Kun virksomheder)
- Oplysninger om forældremyndighed

Opbevaring uden for Danmark

I medfør af bekendtgørelse om lokationskrav nr. 220 af 11. februar 2022 (herefter lokationskravsbekendtgørelsen)[6] 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.

Kravet betyder, 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.

Opbevaring og sletning af oplysninger

Der stilles krav til tidsfrister for sletning af de opbevarede oplysninger om borgere og virksomheder. De fastlagte tidsfrister for opbevaring og sletning af oplysninger for postmeddelelser i Digital Post er følgende:

- Oplysninger om borgeren slettes 5 år efter død jf. § 17, stk. 3 i bekendtgørelse nr. 2019af 29. oktober. 2021 om forvaltning af Digital Post fra offentlige afsendere.
- Oplysninger om virksomheder behandles indtil meddelelserne, efter levering, er overgået til modtagernes råde- og ejendomsret. Det bevirker, at Digitaliseringsstyrelsen opbevarer meddelelser i de digitale postkasser, indtil borgerne eller virksomhederne vælger at slette meddelelserne fra sin digitale postkasse eller efter de generelle sletteregler for Digital Post.

  Af bekendtgørelse nr. 2020 af 29. oktober 2021, om virksomheders § 12, stk. 2, fremgår det, at Digitaliseringsstyrelsen ikke sletter oplysningerne efter leveringen af meddelelsen.

Ud over de nævnte frister kan borgere og virksomheder altid selv slette postmeddelelser i den digitale postkasse.

Sletning af personoplysninger for offentlige afsendere

Alle offentlige afsendere er i henhold til § 2 a, stk. 3 i bekendtgørelsen om offentlige afsendere forpligtede til at indføre et modtagesystem. Modtagesystemet anvendes til opbevaring af meddelelser, som den pågældende offentlige afsender modtager og sender via Digital Post. Dette medfører, at Digitaliseringsstyrelsen ikke opbevarer meddelelser på vegne af offentlige afsendere, når disse er modtaget af den offentlige afsender.

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 opbevarer egne meddelelser i eget modtagersystem, og Digital Post dermed ikke længere opbevarer meddelelser.

Digitaliseringsstyrelsen sletter ikke de omfattede personoplysninger, da meddelelserne efter levering er overgået til modtagernes råde- og ejendomsret. Det bevirker, at Digitaliseringsstyrelsen opbevarer meddelelser i de digitale postkasser, indtil borgerne eller virksomhederne vælger at slette meddelelsen fra sin digitale postkasse eller efter de generelle sletteregler for Digital Post.

[6] 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.

Risikovurdering og notat om risici

Digitaliseringsstyrelsen har som dataansvarlig udarbejdet en risikovurdering i tilknytning til forvaltning af administrationsdata i den driftstekniske del af Digital Post. På baggrund af identificerede risici har Digitaliseringsstyrelsen fastlagt et sikkerhedsniveau for implementering af tekniske og organisatoriske foranstaltninger.

I medfør af bekendtgørelsernes § 6, stk. 1 stiller Digitaliseringsstyrelsen en sammenfatning af den foretagne risikovurderingen til rådighed for de dataansvarlige på Digitaliseringsstyrelsens hjemmeside. Notatet er udformet, så der tages hensyn til, at Digital Post er et samfundskritisk infrastruktursystem i Danmark.

I rollen som dataansvarlig har Digitaliseringsstyrelsen udarbejdet en konsekvensanalyse for behandling af personoplysninger i Digital Post i samarbejde med Kammeradvokaten. Konsekvensanalysen har til formål at identificere og evaluere risici samt at pege på implementering af mulige begrænsende foranstaltninger ved 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, at 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 på vegne af de dataansvarlige. I tidligere nævnte notat om risici har Digitaliseringsstyrelsen listet forskellige scenarier af identificerede risici, som er forbundet med behandling af personoplysninger. Håndtering og begrænsning af de pågældende scenarier er beskrevet 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 mulig begrænsning af risici, såfremt det vurderes nødvendigt.

Tilsynsindsats og kontroller med Digital Post

Beskrivelse af arbejdsform for tilsynet og den praktiske gennemførsel af tilsynsaktiviteter med persondatasikkerheden i Digital Post.

Under dette kapitel beskrives omfang, metode og kontrolaktiviteter for det gennemførte tilsyn med informations- og persondatasikkerhed i Digital Post. Ligeledes beskrives valg af kontroller og dokumentation for tilsynsarbejdet.

Som supplerende information er der tilføjet en uddybende beskrivelse af tre udvalgte kontrolområder, som omhandler brud på persondatasikkerheden, revisionserklæringer fra leverandør og tilsynsrapport fra departementet.

2024 kontrolaktiviteter og resultater fra udført tilsyn med behandling af personoplysninger i Digital Post for perioden 2023 fremgår af kontrolkatalog sidst i redegørelsen.

Omfanget af tilsynet

Digitaliseringsstyrelsen har en rolle som databehandler og dataansvarlig ved behandling af personoplysninger i Digital Post. Tilsynet påser derfor, om Digitaliseringsstyrelsen har etableret en betryggende styring og systemforvaltning af Digital Post i overensstemmelse med de databeskyttelsesretlige forpligtelser.

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 den danske databeskyttelseslov.

Tilsynet tager afsæt i Digitaliseringsstyrelsens ansvar for personoplysninger og informationssikkerhed, som påhviler ved behandling af personoplysninger i Digital Post på vegne af de dataansvarlige jf. Digital Post-loven og bekendtgørelserne.

I praksis betyder tilsynet, at Digitaliseringsstyrelsen skal tilse og vurdere, om beskyttelsen af personoplysninger og informationssikkerhed i Digital Post foregår pålideligt og sikkerhedsmæssigt forsvarligt, så oplysningernes fortrolighed, integritet og tilgængelighed sikres i nødvendigt omfang. Herunder hører også ansvaret for kontraktstyring af underleverandører og løsning af forvaltningsopgaver med udvikling, drift og vedligehold af Digital Post hos underleverandører.

Ligeledes omfatter tilsynet indhentning af supplerende informationer, der berører emner om persondatasikkerhed i Digital Post. Hensigten med dette er at opnå et fyldestgørende vurderingsgrundlag af Digitaliseringsstyrelsens varetagelse af persondatabeskyttelse og den understøttende informationssikkerhed.

Metode for udført tilsyn

Tilsynet er gennemført i dialog mellem Digitaliseringsstyrelsens kontor med ansvar for tilsynsopgaver og kontor med ansvar for Digital Post.

Det udførte tilsyn dækker en kombination af tre tilsynsmetoder.

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.

Vurderingsgrundlaget 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.

De udførte tilsynshandlinger er opdelt efter følgende tre organisatoriske forretningsområder i Digitaliseringsstyrelsen:

1) Ledelsesstyring med informations- og persondatasikkerhed; fx overordnede politikker, procedurer og kontroller i organisationen
2) Kontor med ansvar for vedligehold, udvikling og forvaltning af den digitale postløsning, 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. Det ansvarlige kontor har leveret oplysninger og dokumentation i tilknytning til kontrolmål.

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

Information om brud på persondatasikkerheden

Ifølge § 11 stk. 2 i bekendtgørelserne skal Digitaliseringsstyrelsen, som databehandler, underrette de dataansvarlige offentlige afsendere og virksomheder indenfor 48 timer efter kendskab til brud på persondatasikkerheden. Tidsfristen skal sikre Digitaliseringsstyrelsens bistand til de dataansvarlige, så de dataansvarlige har mulighed for at overholde egne forpligtelser til anmeldelse af brud på persondatasikkerheden til Datatilsynet senest 72 timer efter kendskab til bruddet, jf. databeskyttelsesforordningens artikel 33.

Digitaliseringsstyrelsen har etableret procedurer for rapportering, registrering og håndtering af opfølgning vedrørende brud på informations- og persondatasikkerheden med underdatabehandlere og i forhold til anmeldelser til Datatilsynet.

Brud på persondatasikkerheden i 2023

I 2023 har Digitaliseringsstyrelsen modtaget informationer om fem sikkerhedsbrud, som har haft betydning for behandling af personoplysninger i Digital Post. Hændelserne er anmeldt til Datatilsynet, som endnu ikke har afsluttet håndteringen heraf.

Hændelserne hang primært sammen med komplikationer ved borgeres adgange i løsningen, manglende genlevering af fejlede meddelelser hos modtager, samt utilgængelighed i forbindelse med DDoS-angreb.

En enkel hændelse handlede om en borgerservicemedarbejders sletning af en borgers læseadgang. I dette tilfælde blev det konstateret, at en anden læseadgang end den tiltænkte i stedet kunne blive slettet. Det betød, at en eksisterende læseadgang blev fjernet, mens en ønsket sletning af læseadgang forblev aktiv. Her var Digitaliseringsstyrelsen dataansvarlig.

Desuden blev flere brugere i forbindelse med release af en ny version, ved en fejl afmeldt Digital Post. Myndighederne kunne dermed ikke kontakte disse via Digital Post, men måtte alternativt kontakte de pågældende via fysisk post.

I samme ombæring blev flere borgere bosat i Grønland utilsigtet tilmeldt Digital Post, hvilket tillod myndighederne at sende Digital Post til borgerne. Dette skete til trods for, at borgerne i Grønland ikke er omfattet af lov om Digital Post fra det offentlige. I begge sager var Digitaliseringsstyrelsen dataansvarlig.

Derudover blev der registreret et brud, hvor en modtager havde et modtagersystem, der fejlede, hvilket betød, at

meddelelser ikke blev gensendt, men markeret som leveret. Dette til trods for at meddelelserne aldrig kom frem til modtageren eller blev tilgængelige via Virk.dk.

I forbindelse med et DDOS-angreb var Digital Post-løsningen i kortere tid utilgængelig for alle brugere. Angrebet resulterede ikke i brud på integritet eller fortrolighed, men bevirkede, at løsningen i denne periode ikke kunne tilgås af borgere, virksomheder eller myndigheder.

I forbindelse med alle de nævnte hændelser har Digitaliseringsstyrelsen straks begrænset skadesomfanget og sikret permanente løsninger for at undgå lignende fremtidige hændelser. Ydermere blev relevante borgere, myndigheder og virksomheder hurtigst muligt underrettet om hændelserne. Hændelserne blev ligeledes anmeldt til Datatilsynet.

Information om revisionserklæringer

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

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

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

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

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

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

Revisionserklæringer for 2023 fra underleverandøren

Netcompany har samlet set leveret fire revisionserklæringer for perioden 2023, som er fordelt på to sæt erklæringer, der er adresseret til henholdsvis alle Netcompanys kunder og specifikt til Digitaliseringsstyrelsen for Digital Post. Det skal bemærkes, at kun de to specifikke revisionserklæringer om Digital Post stilles til rådighed for de dataansvarlige.

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

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

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

Foruden en enkelt mindre bemærkning har revisor ikke konstateret mangler ved systemrevisionen, som har givet anledning til forbehold eller bemærkninger og dermed påvirket konklusionen af 2023 revisionserklæringerne. Revisors konklusion i de fire leverede erklæringer viser således, at implementering og kontroller i alle væsentlige henseender er tilfredsstillende samt effektive for at give høj grad af sikkerhed.

Foruden tilsyn med hovedleverandøren Netcompany gennemføres et tilsyn med underleverandører som behandler personoplysninger i forbindelse med delopgaver til den digitale post-løsning. På

Digitaliseringsstyrelsens hjemmeside fremgår listen over underleverandører.

Information om departementets it-tilsynsrapport

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

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

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

Departementets 2024 tilsynsrapport om Digitaliseringsstyrelsen

Digitaliserings- og Ligestillingsministeriets departement har i marts 2024 afgivet den årlige it-tilsynsrapport om det afsluttede tilsyn med informationssikkerhed i Digitaliseringsstyrelsen for 2023.

Af konklusionen fremgår det, at *"Digitaliseringsstyrelsens ledelse har tilrettelagt en styring, der sikrer, at informationssikkerheden er fastlagt og håndteret hensigtsmæssigt, pålideligt og sikkerhedsmæssigt forsvarligt. Dermed sikres informationernes fortrolighed, integritet og tilgængelighed i overensstemmelse med risikoen og det regelgrundlag, styrelsen er underlagt."*

Kontrolkatalog og kontrolmål

Til brug for gennemførsel af tilsynsaktiviteterne anvendes et kontrolkatalog. Kataloget består af en række fastlagte kontrolmål, der dækker krav ved behandling af personoplysninger ifølge §§ 4-12 i bekendtgørelserne om Digital Post. Kontrolmålene er fastlagt med bistand fra Kammeradvokaten ud fra en risikobaseret tilgang og med afsæt i standarderne for 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 vejledninger.

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

Kataloget danner grundlaget for Digitaliseringsstyrelsens dokumentation for efterlevelse af de pågældende krav og etablering af procedurer herfor. Resultatet af det afsluttede tilsyn for perioden 2023 fremgår således i detaljer af indsat kontrolkatalog sidst i redegørelsen.

Kontrolkatalog for 2024 tilsyn med Digital Post

Nedenstående skema udgør dokumentation for resultatet af det afsluttede tilsyn i 2024 med persondatasikkerheden i Digital Post for perioden 2023.

§ 4 Databehandleren handler efter instruks				
Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolmål	Udført test	Testresultat
1.1	**§ 4 Databehandleren handler efter instruks** 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 de dataansvarliges instruks eller ændringer i databehandlingen. Ad B) Konstateret, at procedurer internt i Digitaliseringsstyrelsen og hos underleverandør er opdateret på baggrund af resultat af review og vurdering. 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 fra de dataansvarlige offentlige afsendere og juridiske enheder. 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 de 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) Undersøgt om ledelsen sikrer, at behandling af personoplysninger foregår i henhold til den eventuelle supplerende instruks fra de dataansvarlige. Ad D) Undersøgt om behandlinger af personoplysninger foregår i overensstemmelse med den supplerende instruks fra de dataansvarlige.	Modtaget oplysninger om, at der på baggrund af en juridisk afklaring er etableret en formel proces for håndtering af supplerende instruks fra de dataansvarlige. 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	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 underskrevne kontraktuelle aftaler om lokationskrav.	Ad A) Noteret, at Digitaliseringsstyrelsen har opdaterede fortegnelser over behandlingsaktiviteter med angivelse af, at behandlingen foregår i Danmark. Ad B) Konstateret, at der udføres review og vurdering af procedurer og retningslinjer for behandling samt opbevaring af data på lokationer i Danmark. Ad C) Konstateret, at der fremgår godkendte leverandører i databehandleraftalen mellem Digitaliseringsstyrelsen og underleverandør.	Ingen afvigelser konstateret.

	og opbevaringen af personoplysninger skal ske i Danmark på baggrund af 1. pkt.		Ad C) Undersøgt, at der foreligger underskrevne 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.	
§ 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 ansatte i Digitaliseringsstyrelsen, konsulenter og andre, der bistår styrelsen. 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.	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 i rollen som databehandler har offentliggjort et selvstændigt notat om risici til de dataansvarlige, som tager afsæt i resultater fra risikovurderingen og konsekvensanalysen af Digital Post. 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.	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 awareness-aktiviteter, 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	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 awarenessaktiviteter, 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.

		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.		
§ 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 underdatabehandleraftaler 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 underdatabehandleraftale 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.**	A) Det skal sikres, at kontrakter og aftaler med tredjepartsleverandører er juridisk bindende og leverandø-	Ad A) Noteret, at Digitaliseringsstyrelsen har etableret processer, som sikrer, at kontrakter og aftaler med tred-	Ingen afvigelser konstateret.

	Digitaliseringsstyrelsen sørger for at pålægge underdatabehandlere de samme databeskyttelsesforpligtelser, som dem, der er fastsat ved denne bekendtgørelse, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i henholdsvis databeskyttelsesforordningen eller retshåndhævelsesloven. 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.	rerne pålægges at overholde Europæisk og dansk lovgivning herunder bl.a. supplerende databeskyttelsesregler og bekendtgørelser. 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.	jepartsleverandører 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 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 årligt 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 databeskyttelses-	A) Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren kun overfører personoplysninger til tredjelande efter aftale 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	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.

	forordningens 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).	tredjelande, herunder hvilke oplysninger 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, at Digitaliseringsstyrelsens procedurer vedrørende bistand til de dataansvarlige, herunder offentliggørelse af informationer på hjemmeside om Digital Post, 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 dataansvarlig skal sikre overholdelsen af nedenstående regler i databeskyttelsesforordningen og retshåndhævelsesloven:	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. B) Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand	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. 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.	Ingen afvigelser konstateret.

	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.	til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Ad B) Noteret, at der findes diagram med dataflow, og at 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 af, 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 rettidigt kan underrette den dataansvarlige og bistå med information om bruddet på persondatasikkerheden, så den dataansvarlige kan foretage vurdering af, om der skal ske anmeldelse til Datatilsynet indenfor 72 timer. C) Der foreligger et skriftligt overblik vedrørende opfølgning og status på årets relevante databeskyttelsesmæssige hændelser. 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, sandsynlige konsekvenser af bruddet på persondatasikkerheden samt mulige foranstaltninger til håndtering af bruddet. Ad B) Konstateret, at der foreligger kontraktkrav og en 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 fem brud på persondatasikkerheden til Datatilsynet i 2023 og at relevante borgere, myndigheder og virksomheder samtidigt er underrettet om hændelserne. Ad D) Noteret, at Digitaliseringsstyrelsen løbende – og mindst en gang årligt – opdaterer procedurer og retningslinjer vedrørende håndtering af sikkerhedshændelser.	Det er oplyst, at der fortsat udestår tilbagemelding fra Datatilsynet på fem anmeldte hændelser. Ingen yderligere afvigelser konstateret.
Nr.	Forpligtelser jf. bekendtgørelserne	Kontrolmål	Udført test	Testresultat
5.5	**§ 10 Bistand til den dataansvarlige** Stk. 3. nr. 4. (Gennemførelse af konsekvensanalyse)	A) Der foreligger skriftlige procedurer, som sikrer, at databehandleren rettidigt underretter den dataansvarlige, når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for de registreredes rettigheder.	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 et brud sandsynligvis vil indebære en høj risiko for de registreredes rettigheder.	Ingen afvigelser konstateret.

	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.	B) Der foreligger krav og procedurer, der sikrer, at databehandleren kan bistå med information om bruddet på persondatasikkerheden, så den dataansvarlige kan foretage vurdering af, om de registrerede skal underrettes. Ad C: Der skal foretages løbende – og mindst en gang årligt – vurdering og opdatering af procedurer vedr. underretning.	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.	
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 procedurer, som indeholder krav om og beskriver, hvordan databehandleren rettidigt skal bistå den dataansvarlige med at sikre overholdelse af forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse. B) Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. C) Digitaliseringsstyrelsen har på sin hjemmeside offentliggjort relevant materiale, som bistand til de dataansvarliges arbejde med egen konsekvensanalyse samt valg af foranstaltninger til begrænsning af risici, såfremt det vurderes nødvendigt.	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) Noteret, at Digitaliseringsstyrelsen løbende – og mindst en gang årligt – vurderer om procedurer skal opdateres. Ad C) Noteret, at Digitaliseringsstyrelsen i rollen som databehandler har offentliggjort et selvstændigt notat om risici, som bistand til de dataansvarliges arbejde med egen konsekvensanalyse samt valg af foranstaltninger til begrænsning af risici, såfremt det vurderes nødvendigt.	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 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.	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 bistår de dataansvarlige med information om bl.a. karakteren, 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 indenfor 48 timer, når der er konstateret sandsynlighed for brud på persondatasikkerheden. Ad B) Konstateret, at der foreligger kontraktkrav og en underdatabehandleraftale med underleverandøren, som sikrer, at der er etableret procedurer for bistand til Digitaliseringsstyrelsen ved underretning til de dataansvarlige indenfor 48 timer og anmeldelse til Datatilsynet senest 72 timer, herunder evt. underretningsbrev om karakteren af bruddet, konsekvenser og mulige foranstaltninger til håndtering af bruddet. Ad C) Noteret, at Digitaliseringsstyrelsen løbende – og mindst en gang årligt – opdaterer procedurer og retningslinjer vedrørende håndtering af brud på persondatasikkerheden.	Ingen afvigelser konstateret.

	3) [De foranstaltninger, som Digitaliseringsstyrelsen har udført som databehandler]			
§ 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 Digitaliseringsstyrelsen har indhentet revisionsbevis fra underleverandøren for overholdelse af krav til opbevaringsperiode og sletterutiner for meddelelser i de digitale 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.

Digitaliserings-
styrelsen