



Høringsnotat om udkast til

16. september 2021
JUR/DNA/mofis
J.nr. 2019 – 4329

1) bekendtgørelse om ansvar, opgaver og tilsyn for behandlingen af personoplysninger i forbindelse med forsendelse af digital post fra offentlige afsendere

og

2) bekendtgørelse om ansvar, opgaver og tilsyn for behandlingen af personoplysninger indeholdt i meddelelser og opbevaringen heraf i juridiske enheders digitale postkasse

1.	Indledning	3
2.	Sammenfatning af ændringer i lovforslaget i forhold til høringsudkastet 4	
3.	Generelle bemærkninger til lovudkastet	6
4.	Bemærkninger til udkastenes temaer	7
3.1	Krav til databehandleraftaler	7
3.2	Om Digitaliseringsstyrelsens databehandling	8
3.3	Kategorier af personoplysninger	11
3.4	Databehandleren handler efter instruks	12
3.5	Videregivelse til statistiske eller videnskabelige undersøgelser.....	13
3.6	Metadata	14
3.7	Fortrolighed.....	14
3.8	Behandlingssikkerhed.....	15
3.9	Anvendelse af underdatabehandlere	17
3.10	Overførsel til tredjelande eller internationale organisationer	20
3.11	De registreredes rettigheder og sletning af personoplysninger.....	24
3.12	Konsekvensanalyse.....	25
3.13	Underretning om brud på persondatasikkerhed til Datatilsynet	27
3.14	Tilsyn og revision.....	29
3.15	Offentlige afsendere	32
3.16	Retshåndhævende myndigheder.....	34

1. Indledning

1) Udkast til bekendtgørelse om ansvar, opgaver og tilsyn for behandlingen af personoplysninger i forbindelse med forsendelse af digital post fra offentlige afsendere

og

2) udkast til bekendtgørelse om ansvar, opgaver og tilsyn for behandlingen af personoplysninger indeholdt i meddelelser og opbevaringen heraf i juridiske enheders digitale postkasse

har i perioden fra den 11. december 2020 til den 5. februar 2021 været i ekstern høring hos 68 myndigheder og organisationer. Udkastene blev også offentliggjort på Høringsportalen.

Der er modtaget høringssvar fra 21 af de hørte myndigheder og organisationer. 15 høringssvar indeholder bemærkninger til bekendtgørelserne. En oversigt over, hvilke af de hørte myndigheder og organisationer, der har afgivet høringssvar, er indsat nedenfor.

De væsentligste bemærkninger fra høringssvarene er medtaget i dette notat.

Dato	Afsender	Bemærkninger
02-02-2021	Børne- og Undervisningsministeriet - STIL	Nej
14-12-2021	Dansk Arbejdsgiverforening	Nej
05-02-2021	Datatilsynet	Ja
04-02-2021	Domstolsstyrelsen	Ja
04-02-2021	Erhvervsministeriet - Nævnenes Hus	Ja
04-02-2021	Forsikring og Pension	Ja
04-02-2021	Forsvarsministeriet - Forsvarsministeriets Personalestyrelse	Ja
05-02-2021	Forsvarsministeriet og Forsvarsministeriets Auditørkorps	Ja
19-01-2021	FSR – danske revisorer	Ja
04-02-2021	Grønlands Selvstyre	Nej
08-02-2021	Institut for Menneskerettigheder	Ja

05-02-2021	KL (ny)	Ja
05-02-2021	Miljøministeriet	Nej
05-02-2021	Region Hovestaden	Ja
05-02-2021	Region Midtjylland	Ja
05-02-2021	Region Nordjylland	Ja
05-02-2021	Region Syddanmark	Ja
21-01-2021	Socialstyrelsen	Ja
08-02-2021	Sundhedsministeriet	Nej
05-02-2021	Uddannelses- og Forskningsministeriet	Ja
28-01-2021	ÆldreSagen	Nej

2. Sammenfatning af ændringer i bekendtgørelserne i forhold til høringsudkastet

De indkomne høringssvar har givet anledning til følgende ændringer i bekendtgørelses-teksten:

- Henvisninger til retshåndhævelsesloven er generelt tilføjet til bestemmelserne i bekendtgørelsen om offentlige afsendere.
- § 1
 - Henvisningerne til lovgivning og specifikke bestemmelser er præciseret.
- § 2
 - Der er indsat nyt stk. 2, hvorefter de dataansvarliges formål med behandlingen er præciseret. De efterfølgende stykker forrykkes som konsekvens heraf.
 - I det nye stk. 3, er der indsat et 2. pkt. om metadata.
 - I det nye stk. 5, er lovhenviisning præciseret.
- § 3
 - I stk. 1 er der tilføjet eksempler på personoplysninger.
- § 4
 - Tre nye stykker, stk. 1-3, er tilføjet, der forrykker de efterfølgende stykker. Stk. 1-3 udgør instruks for Digitaliseringsstyrelsens databehandling. Herefter er det tidligere stk. 1, blevet til stk. 4.
 - Det oprindelige stk. 2, 4 og 5 udgår.
 - Stk. 5-6 er nye stykker, der oplyser om behandlingen og instruks til Digitaliseringsstyrelsen.



- Det oprindelige stk. 3 er blevet til stk. 7.
- Nyt stk. 8 angiver, at Digital Post-løsningen er omfattet af lokationskravet i databeskyttelseslovens § 3, stk. 9.
- § 6
 - I stk. 1 præciseres det, at Digitaliseringsstyrelsen fastsætter foranstaltninger i medfør af databeskyttelsesforordningens artikel 32 på baggrund af en risikovurdering. Styrelsen stiller en sammenfatning af risikovurderingen til rådighed på sin hjemmeside for de dataansvarlige.
 - I stk. 2 præciseres det, at Digitaliseringsstyrelsen gennemfører passende tekniske og organisatoriske foranstaltninger.
 - Stk. 2, nr. 2, er ændret, så den nu vedrører logning af brug og adgang til personoplysninger.
 - Det oprindelige stk. 3 udgår, og stk. 4 bliver herefter stk. 3, hvor bestemmelsen er præciseret og nr. 3 udgår.
 - Det oprindelige stk. 5 og 6 bliver stk. 4 og 5.
- § 7
 - Stk. 1 og 3 er præciseret.
 - Stk. 4-6 udgår. Det oprindelige stk. 7 bliver herefter til stk. 4, der ligeledes er præciseret, hvorefter kontrol skal ske, når det findes nødvendigt, og mindst én gang hvert år.
- § 8
 - I stk. 1 er der indsat et 2. pkt. om varsling af indsigelsesret ved brug af underdatabehandler.
 - I stk. 6, nr. 1, er det præciseret, at revisorerklæringer skal være i overensstemmelse med aktuelle standarder for GDPR-revisorerklæringer.
- § 9
 - Et nyt stk. 1 er indsat for at præcisere, at Digitaliseringsstyrelsen ikke overfører personoplysninger til tredjelande eller internationale organisationer.
 - Det oprindelige stk. 1-3 bliver herefter til stk. 2-4.
- § 10
 - I stk. 2 er der foretaget en sproglig justering af første del af sætningen uden indholdsmæssig betydning.
- § 11
 - I stk. 3 er der tilføjet et nyt 2. pkt., hvor det fremgår, at Digitaliseringsstyrelsen uden unødig forsinkelse underretter den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden, og inden en samlet anmeldelse sendes til Datatilsynet i medfør af 1. pkt.
 - I stk. 4, nr. 3, er det præciseret, at der menes de foranstaltninger, som Digitaliseringsstyrelsen har udført som databehandler.
- § 12
 - I henholdsvis stk. 1 (bekendtgørelse for offentlige afsendere) og stk. 2 (bekendtgørelse for juridiske enheder) er det præciseret, at meddelelserne efter levering er overgået til modtagernes råde- og ejendomsret.

- § 13
 - I stk. 1 er det præciseret, at det er *alle* relevante og nødvendige oplysninger, der stilles til rådighed for de dataansvarlige.
 - I stk. 3, er der indsat et nyt 2. pkt., hvorefter de dataansvarlige har mulighed for at anmode om supplerende oplysninger om Digitaliseringsstyrelsens databehandling, ligesom alle relevante oplysninger vil blive stillet til rådighed for de dataansvarlige på Digitaliseringsstyrelsens hjemmeside.
 - I stk. 4, 2. pkt., er det præciseret, at der *årligt* udarbejdes en tilsynsrapport.
- § 15
 - Ikrafttrædelsesbestemmelsen er ændret fra, at finansministeren fastsætter tidspunktet til, at ikrafttræden er den specifikke dato for omstillingsperioden op til idriftsættelsen af den nye Digital Post-løsning, da den planlagte dato herfor nu foreligger. Dette vil øge transparensen for, hvornår reglerne har retlig virkning, også ud fra et fremtidigt perspektiv.

3. Generelle bemærkninger til lovudkastet

Digitaliseringsstyrelsen bemærker, at de indkomne høringssvar primært relaterer sig til bekendtgørelse om ansvar, opgaver og tilsyn for behandlingen af personoplysninger i forbindelse med forsendelse af digital post fra offentlige afsendere eller begge udkast. I de tilfælde, hvor der specifikt er bemærkninger til udkast til bekendtgørelse om ansvar, opgaver og tilsyn for behandlingen af personoplysninger indeholdt i meddelelser og opbevaringen heraf i juridiske enheders digitale postkasse, vil dette fremgå eksplicit.

Institut for Menneskerettigheder oplyser, at de kan se det praktiske i at erstatte databehandlingsaftaler mellem Digitaliseringsstyrelsen og samtlige dataansvarlige med én samlet bekendtgørelse, men udtrykker tvivl om, hvorvidt bekendtgørelserne vil sikre databeskyttelsen og datasikkerheden tilstrækkeligt i alle situationer.

KL ser meget positivt på, at denne type databehandlersaftaler mellem staten og kommunerne indgås via bekendtgørelser. Det medvirker ifølge KL til, at den enkelte kommune ikke skal anvende unødige resurser på at forholde sig til databehandlersaftaler med staten, som de efter KL's opfattelse har begrænset reel indflydelse på, jf. lov nr. 1941 af 15. december 2020, § 2 a, stk. 5, hvorefter "Finansministeren kan fastsætte regler om ansvar, opgaver og tilsyn i forbindelse med Digitaliseringsstyrelsens behandling af personoplysninger i postløsningen på vegne af de dataansvarlige, jf. stk. 3 og 4." Anvendelsen af bekendtgørelsesformen letter kommunernes administrative arbejde.

KL mener desuden, at det er en stor hjælp, at bekendtgørelserne er udarbejdet med afsæt i Datatilsynets standardkontraktbestemmelser. Det medvirker til genkendelighed og dermed lettere anvendelse af reglerne for kommunerne.

Region Hovedstaden finder det meget positivt, at kravene til databehandlingen i Digital Post-løsningen reguleres via bekendtgørelser i tråd med mulighederne i databeskyttelsesforord-

ningens artikel 28 stk. 3. Dette letter generelt offentlige myndigheder og dermed også regionens arbejde med at afklare og fastlægge de juridiske rammer for den nye Digital Post-løsning betragteligt og kan ifølge Region Hovedstaden med fordel danne præcedens i forhold til andre fællesoffentlige digitaliseringsprojekter, hvor den samme løsning benyttes på tværs af aktørerne i den offentlige sektor. Regionen finder det ligeledes positivt, at bekendtgørelserne forholder sig til og dækker både rolle- og ansvarsfordeling i forhold til tilsyn og brud på persondatasikkerheden, hvilket formodes at lette regionens processer og sagsbehandling, når løsningen går i drift.

Region Midtjylland ser det som en god ide at udstede de to bekendtgørelser, så Digitaliseringsstyrelsens rolle som databehandler er fastlagt. Region Midtjylland har dog trods alt nogle tekstmære bemærkninger til de to bekendtgørelser baseret på, hvad bekendtgørelsen giver af mulighed for at efterleve forordningen for Region Midtjylland som dataansvarlig. Disse vil komme til udtryk længere nede i høringsnotatet.

Region Syddanmark oplyser, at de overordnet bifalder forslagene til de to bekendtgørelser. Regionen finder det værdifuldt, at Digitaliseringsstyrelsens rolle og ansvar som databehandler nu bliver præciseret, som en uddybning af Digital Post loven. Regionen vurderer, at bekendtgørelserne generelt lever op til vilkårene i databeskyttelsesforordningen, og opfylder de behov, offentlige myndigheder har i forhold til Digitaliseringsstyrelsens rolle som databehandler.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen har noteret sig den positive modtagelse af udkastene til bekendtgørelserne.

4. Bemærkninger til udkastenes temaer

3.1 Krav til databehandleraftaler

Datatilsynet gengiver databeskyttelsesforordningens artikel 28, stk. 3, litra a-h og understreger, at det er en forudsætning, at kontrakten eller det retlige dokument som minimum opfylder alle disse krav.

Region Midtjylland bemærker til bekendtgørelsens § 1, stk. 2, 2. pkt., at der er visse standardkontraktbestemmelser fra blandt andet Datatilsynet, som denne bekendtgørelse skal indeholde jf. databeskyttelsesforordningen artikel 28, stk. 6-8. Høringsbrevet indikerer, at Digitaliseringsstyrelsen er opmærksom herpå, men for god ordens skyld forventes det, at disse standardkontraktbestemmelser er indarbejdet i denne bekendtgørelse.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen tager bemærkningerne til efterretning og tilpasser bekendtgørelserne i overensstemmelse hermed, således at disse krav opfyldes.

Region Midtjylland bemærker til bekendtgørelsens § 2, at det er regionens vurdering, at de dataansvarliges formål med databehandlingen ikke er beskrevet i § 2. Formålet skal beskrives i denne bestemmelse, så det er i overensstemmelse med kravet herom for blandt andet et retligt dokument i databeskyttelsesforordningens artikel 28, stk. 3.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen tager bemærkningen til efterretning og tilpasser bekendtgørelserne i overensstemmelse hermed.

Region Midtjylland bemærker til bekendtgørelsen § 2, stk. 3, at regionen efterspørger en instruks, hvor databehandlerens ansvar/forpligtelse i forbindelse med databehandlingen fremgår.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen har i bekendtgørelsens § 4 indskrevet den af Region Midtjylland efterspurgte instruks, og vil derfor ikke tilpasse § 2, stk. 3. Instruksen præciseres i øvrigt yderligere, hvilket fremgår af svar til afsnit 3.4 nedenfor.

Region Syddanmark bemærker, at i formuleringen i høringsbrevet om, at bestemmelsen i praksis giver ministeren hjemmel til i bekendtgørelsesform at fastsætte vilkårene for Digitaliseringsstyrelsens databehandling, savner Region Syddanmark en præcisering af, hvad der ligger i at give denne hjemmel til ministeren. Er det normal praksis, at databehandleren selv kan fastsætte vilkår for behandling?

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen har på vegne af de offentlige afsendere gennemført et udbud af Digital Post-løsningen. Udbuddet har medført, at Digitaliseringsstyrelsen hjemtager dataansvaret for løsningen, hvilket også indebærer en ændring af databehandlerkonstruktionen. I stedet for at pålægge de offentlige afsendere at indgå et større antal databehandleraftaler har lovforslaget muliggjort at finansministeren i bekendtgørelsesform fastsætter vilkårene for databehandlingen. Digitaliseringsstyrelsen er ikke bekendt med lignende hjemler i lov, men kender til cirkulæreskrivelser såvel som aftaler om fælles dataansvar, hvor databehandling fastlægges. Se CIS nr. 9962 af 05/11/2019, Cirkulæreskrivelse om Styrelsen for It og Læringsopgaver som databehandler i det digitale system Sprogprøver.dk og CIS nr. 9223 af 23/03/2018, Cirkulæreskrivelse om fælles dataansvar vedrørende Moderniseringsstyrelsens fællesoffentlige systemer.

3.2 Om Digitaliseringsstyrelsens databehandling

Nævnenes Hus bemærker til § 4 i bekendtgørelse om ansvar, opgaver og tilsyn for behandlingen af personoplysninger i forbindelse med forsendelse af digital post fra offentlige afsendere, at Nævnenes Hus er i tvivl om, hvorvidt Digitaliseringsstyrelsen anser sig selv for databehandler efter levering af en meddelelse, og hvis det ikke er tilfældet, om det så skyldes, at der ikke længere sker databehandling?

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen kan bekræfte, at styrelsen ikke ser sig selv som databehandler for offentlige afsendere efter levering af en meddelelse til en borger. Dette skyldes, at Digitaliseringsstyrelsen bliver dataansvarlig for den tekniske opbevaring af meddelelserne i borgerens postkasse. Borgeren er som udgangspunkt ikke omfattet af anvendelsesområdet for databeskyttelsesforordningen, jf. artikel 2, stk. 2, litra c, og dermed ikke dataansvarlig i databeskyttelsesretlig forstand for den digitale post i dennes egen digitale postkasse, uanset om denne post eventuelt måtte indeholde personoplysninger om tredjeparter. Borgeren er desuden den eneste med råde- og ejendomsret over egen digital post.

For en virksomhed gælder det derimod, jf. § 4, stk. 3, i udkast til bekendtgørelse om ansvar, opgaver og tilsyn for behandlingen af personoplysninger indeholdt i meddelelser og opbevaringen heraf i juridiske enheders digitale postkasse, at styrelsen bliver databehandler for opbevaringen af meddelelserne i virksomhedens postkasse, idet virksomheden selv er dataansvarlig for sin post.

Institut for Menneskerettigheder bemærker, at de er i tvivl om, hvorvidt styrelsen udelukkende kan anses for databehandler, da de respektive afsendere ifølge instituttet næppe alene ”afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger” i relation til Digital Post, jf. forordningens artikel 4, stk. 7, eller om styrelsen reelt er fælles dataansvarlig med afsenderne.

Selvom bekendtgørelserne bygger på Datatilsynets standardkontrakt, kan dette ifølge Institut for Menneskerettigheder føre til uklarheder omkring den reelle ansvarsfordeling mellem styrelsen og afsenderne, herunder i relation til efterlevelsen af databeskyttelsesprincipperne i forordningens artikel 5 og den registreredes rettigheder i artikel 12 mv.

Sådanne uklarheder kan ifølge Institut for Menneskerettigheder stille borgere, der modtager Digital Post, i en vanskelig situation, da det kan blive vanskeligt for dem at føre kontrol med behandlingen af deres personoplysninger efter forordningen, hvilket kan betyde en forringet beskyttelse af borgerens personoplysninger efter forordningen og EU-Chartrets artikel 8. Institut for Menneskerettigheder anbefaler, at der udarbejdes en vejledning om Digitaliseringsstyrelsens databehandling (og eventuelt fælles dataansvar) i relation til Digital Post for offentlige afsendere og juridiske enheder, så ansvarsfordelingen står borgerne klart, med henblik på at de kan udnytte deres rettigheder efter forordningen.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen har følgende bemærkning til spørgsmålet om, hvorvidt der bør være fælles dataansvar mellem de offentlige afsendere og styrelsen:

Når en offentlig myndighed sender Digital Post, er myndigheden dataansvarlig for indholdet af meddelelsen. Dataansvaret overgår ikke til Digitaliseringsstyrelsen, hvorfor myndigheden til stadighed vil være dataansvarlig for indholdet, af de meddelelser som sendes igennem løsningen. Meddelelserne kan have retsvirkninger for borgerne, idet de f.eks. kan indeholde

afgørelser, tilladelser, afslag mv. Den offentlige myndighed kan erstatte en afsendt meddelelse, ved at sende en ny, der giver borgeren eller virksomheden en anden retsstilling. Digitaliseringsstyrelsen har hverken indflydelse på, hvornår disse meddelelser afsendes, eller på indholdet, idet det henhører under afsendermyndighedens ressort.

Digitaliseringsstyrelsen har således ingen indflydelse på formålet med behandlingen af personoplysninger i forbindelse med myndighedernes afsendelse af Digital Post. Digitaliseringsstyrelsen giver heller ikke de offentlige myndigheder en instruks for deres anvendelse af postløsningen, da den blot stilles til deres rådighed med mulighed for benyttelse. Dét forhold, at postløsningen benyttes til langt de fleste afsendelser af meddelelser fra offentlige myndigheder, ændrer ikke derved.

Digitaliseringsstyrelsen bliver dermed kun databehandler for den tekniske levering af digital post i forsendelsessituationen, mens den offentlige myndighed, der sender digital post gennem postløsningen, er dataansvarlig for, at indholdet af den digitale post er juridisk korrekt og leveret til den rette modtager.

Såfremt meddelelsen i forsendelsesøjeblikket stiles til den forkerte modtager, er den myndighed, der sender digital post, dataansvarlig for dette og skal dermed vurdere, om Datatilsynet eventuelt skal underrettes om sikkerhedsbruddet. Den dataansvarlige myndighed skal ligeledes vurdere, om den registrerede, der eventuelt har fået delt sine personoplysninger med en forkert modtager, skal orienteres. Afsendermyndigheden er den eneste til at vurdere dette, og Digitaliseringsstyrelsen bliver dermed ikke dataansvarlig for om meddelelsen - og indholdet heraf – sendes til den rette modtager eller ej.

De offentlige myndigheder bliver således – som i dag – dataansvarlige for forsendelser, som de sender gennem den nye løsning, og Digitaliseringsstyrelsen bliver databehandler for de offentlige myndigheders forsendelse.

I relation til spørgsmålet om at udstede en vejledning, kan Digitaliseringsstyrelsen oplyse, at dette tages til overvejelse. Det bemærkes, at Digitaliseringsstyrelsen med Digital Post-løsningen har stort fokus på at opfylde de registreredes rettigheder, og som dataansvarlige for Digital Post vil bidrage til at håndtere henvendelser fra de registrerede i rollen som databehandler for de offentlige afsendere og juridiske enheder.

Region Hovedstaden vurderer, at der ligger et potentiale i at overveje andre konstruktioner i forbindelse med fællesoffentlige digitale løsninger og andre typer af samarbejde mellem offentlige myndigheder, end bekendtgørelserne her lægger op til. Det kan f.eks. være lovlig videregivelse eller fælles dataansvar. I det omfang, at det er meningsfuldt at lovgive i de konkrete sammenhænge, vil regionen se positivt på en øget anvendelse af lovgivning, som overordnet ramme, da de administrative opgaver, der er forbundet med en klassisk databehandlerkonstruktion hermed mindskes. Dertil kommer, at disse overvejelser vil være med til at modne offentlige myndigheders arbejde med at fastlægge modeller for roller og ansvar for databehandling på tværs af den offentlige sektor i almindelighed.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen bemærker til overvejslen om fælles dataansvar, at styrelsen har redegjort for databehandlerkonstruktionen ovenfor og henviser hertil. Digitaliseringsstyrelsen er enig i at fastlæggelse af roller og ansvar kan mindske myndighedernes administrative opgaver forbundet med databehandling.

Region Syddanmark bemærker til høringsbrevet, at det oplyses, at bekendtgørelsen præciserer, at Digitaliseringsstyrelsens databehandling ophører ved levering i modtagerens postkasse. Region Syddanmark ønsker bekræftet, hvorvidt der fortsat, efter regionens opfattelse, sker opbevaring hos Digitaliseringsstyrelsen på borger.dk, hvor borgerens offentlige postkasse ligger, såfremt en borger ikke vælger at benytte sig af en kommerciel visningsklient. Regionen spørger, om opbevaring ikke er en behandling, som Digitaliseringsstyrelsen foretager på vegne af de dataansvarlige efter levering i borgerens digitale postkasse?

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen bemærker, at selve opbevaringen af borgernes meddelelse vil ske samme sted i den digitale postløsning, uanset hvilken visningsklient, borgeren vælger, f.eks. den offentlige visningsklient på borger.dk. Borgerens handlinger i vedkommendes postkasse vil afspejles i hvilken som helst visningsklient, som borgeren anvender, fordi opbevaringen vil ske centralt i postløsningen. Digitaliseringsstyrelsen anser sig som dataansvarlig for den tekniske opbevaring af meddelelser i borgernes postkasser. Borgeren er desuden den eneste med råde- og ejendomsret over egen digital post. Se gerne uddybningen ovenfor.

I relation til opbevaring af meddelelser i en virksomheds postkasse gælder det derimod, at Digitaliseringsstyrelsen bliver databehandler for opbevaringen af meddelelserne i virksomhedens postkasse, idet virksomheden selv er dataansvarlig for sin post, se i øvrigt bekendtgørelse om ansvar, opgaver og tilsyn for behandlingen af personoplysninger indeholdt i meddelelser og opbevaringen heraf i juridiske enheders digitale postkasser.

3.3 Kategorier af personoplysninger

Region Midtjylland foreslår, at bekendtgørelsens § 3, stk. 1, suppleres med eksempler på, hvilke personoplysninger der kan være tale om inden for henholdsvis almindelige personoplysninger, særlige kategorier af personoplysninger (følsomme personoplysninger) i medfør af databeskyttelsesforordningens artikel 9, stk. 1, samt oplysninger om strafbare forhold.

Region Syddanmark bemærker, at § 3, stk. 1 og 2, bør være mere specifikke i forhold til kategorier af registrerede, herunder borgere i Danmark, der er tilmeldt Digital Post og ansatte i offentlige myndigheder i Danmark, der er tilmeldt Digital Post.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen tager bemærkningerne til efterretning og konkretiserer personoplysningerne efter stk. 1 med eksempler, men fortager ikke ændringer i stk. 2, da det allerede af

bestemmelsen fremgår, at både borgere og medarbejdere er omfattet og dermed også ansatte i offentlige myndigheder.

3.4 Databehandleren handler efter instruks

Datatilsynet bemærker, at det er Datatilsynets opfattelse, at udkastets § 4 alene gengiver det forudsatte princip i databeskyttelsesforordningens artikel 28, stk. 3, litra a, om, at databehandleren alene agerer i henhold til instruks og intet siger om instruksens indhold. Det er på den baggrund en forudsætning, at de enkelte dataansvarlige, inden behandlingen påbegyndes, rent faktisk afgiver en sådan instruks til databehandleren.

Forsikring & Pension bemærker, at den dataansvarlige efter databeskyttelsesforordningen har pligt til at give instruks til databehandleren, og at databehandlerne kun må handle efter instruks fra den dataansvarlige. Digitaliseringsstyrelsen bør efter Forsikring & Pensions opfattelse tage nærmere stilling til, hvordan kravet om instruks opfyldes i denne bekendtgørelse.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen bemærker, at instruks i § 4 vil blive præciseret, så den udgør en fyldestgørende databeskyttelsesretlig instruks, der ikke kræver yderligere særskilte instrukser fra de dataansvarlige offentlige afsendere og juridiske enheder.

Region Syddanmark bemærker, at opstillingen i bekendtgørelsernes § 4 bør være ens. Den opstilling, der er i bekendtgørelse om ansvar, opgaver og tilsyn for behandlingen af personoplysninger indeholdt i meddelelser og opbevaringen heraf i juridiske enheders digitale postkasse, giver det bedste overblik, derfor bør den ifølge Region Syddanmark anvendes i begge bekendtgørelser.

Region Syddanmark bemærker til § 4, stk. 2, at Digitaliseringsstyrelsen underretter den offentlige afsender, hvis en instruks efter Digitaliseringsstyrelsens mening er i strid med databeskyttelsesforordningen eller bestemmelser om databeskyttelse i anden EU-ret eller national ret. Regionen spørger, om det ikke er Digitaliseringsstyrelsen, der skriver bekendtgørelsen, herunder instruks – så er dette [overhovedet] en mulighed?

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen bemærker, at behandlingen efter § 4, stk. 1, ikke kan justeres, så de bliver enslydende. Dette skyldes, at Digitaliseringsstyrelsen kun bliver databehandler for offentlige afsendere ved forsendelse af digital post. Digitaliseringsstyrelsen bliver derimod databehandler for såvel forsendelse som opbevaring for de juridiske enheder.

Digitaliseringsstyrelsen har udformet bekendtgørelserne, så de opfylder kravene til at stå i stedet for en databehandleraftale. § 4, stk. 2, er derfor udformet for at opfylde disse krav.



3.5 Videregivelse til statistiske eller videnskabelige undersøgelser

Forsikring & Pension bemærker, at videregivelse af metadata efter databeskyttelseslovens § 10, fra Digital Post til brug for udførelse af f.eks. statistiske eller videnskabelige undersøgelser, efter deres opfattelse kun må ske mod forudgående høring. Det er desuden ikke klart, hvilke data, der omfattes af termen metadata, som dermed kan videregives. Det bør efter Forsikring og Pensions opfattelse præciseres.

KL bemærker, at der i § 4, stk. 4 og 5, lægges op til, at Digitaliseringsstyrelsen bliver selvstændigt dataansvarlig for videregivelsen af metadata fra Digital Post til f.eks. statistiske eller videnskabelige undersøgelser. KL vil anbefale, at disse bestemmelser udgår af afsnittet, "Databehandleren handler efter instruks", eftersom databehandleren i disse tilfælde ikke handler efter instruks.

Desuden bemærker KL, at såfremt metadata ikke er personoplysninger i databeskyttelsesforordningens forstand vil KL anbefale, at § 4, stk. 4 og 5, udgår af bekendtgørelsen, idet disse oplysninger ikke er reguleret af databeskyttelsesforordningen.

Region Nordjylland bemærker til § 4, stk. 4 og 5, at Digitaliseringsstyrelsen i forbindelse med videregivelser i henhold til stk. 4, jf. stk. 5, bliver selvstændig dataansvarlig for de videregivne personoplysninger, og Digitaliseringsstyrelsen er ansvarlig for at sikre, at der er en gyldig hjemmel til videregivelsen mv.

Uddannelses- og Forskningsministeriet foreslår til udkastets § 4, stk. 4, om videregivelse af metadata fra Digital Post efter databeskyttelseslovens § 10, at bestemmelsen udskilles i en selvstændig bestemmelse under en anden overskrift end "Databehandleren handler efter instruks", idet videregivelsen i givet fald ikke sker efter instruks fra den myndighed, der i øvrigt er dataansvarlig for de pågældende oplysninger.

Socialstyrelsen bemærker til § 4, stk. 5, at videregivelse af metadata til Digitaliseringsstyrelsen til brug for formål efter § 10 i databeskyttelsesloven forudsætter erklæring af de lovpligtige punkter i bekendtgørelse om videregivelse omfattet af § 10 i databeskyttelsesloven. Socialstyrelsen spørger, hvorledes den afgivende dataansvarliges forpligtelser samt orientering af de registrerede om videregivelsen sikres.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen bemærker indledningsvist, at styrelsen ikke er enig i Forsikring og Pensions vurdering af, at en videregivelse af data efter § 10 i databeskyttelsesloven kun kan ske mod forudgående høring.

Digitaliseringsstyrelsen har dernæst revurderet behovet for at regulere videregivelsen af data til statistiske eller videnskabelige undersøgelser i bekendtgørelsen, hvorfor disse udgår. Bestemmelserne udgår, fordi Digitaliseringsstyrelsen handler som dataansvarlig myndighed for Digital Post og ikke på vegne af de dataansvarlige offentlige afsendere.

3.6 Metadata

Region Syddanmark ønsker, at bekendtgørelserne klart vil definere begrebet "metadata", og vil derfor anbefale en nærmere præcisering heraf i bekendtgørelserne.

I bekendtgørelsen nævnes i § 4, stk. 4, at Digitaliseringsstyrelsen kan videregive metadata til "brug for udførelse af f.eks. statistiske eller videnskabelige undersøgelser (...)". På baggrund af dette bør § 3, stk. 1, efter regionens opfattelse også nævne metadata, som eksempel på typer af personoplysninger, der kan behandles.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen vil i bekendtgørelserne præcisere, at metadata i denne sammenhæng alene omfatter metadata, som de offentlige afsendere vælger at tilknytte deres meddelelser i forbindelse med afsendelsen og ikke metadata i form af administrationsdata, der muliggør selve leveringen af meddelelserne.

Socialstyrelsen bemærker i relation til § 4, stk. 4, at det ikke af bekendtgørelsen fremgår hvilke data, metadata vedrører? Der kan f.eks. forekomme tilfælde, hvor Socialstyrelsen som dataansvarlig har lovet en modtager af Digital Post fra Socialstyrelsen, at vedkommendes CPR-nummer ikke videregives til andre, men hvor CPR-nummeret er indeholdt i metadata. Socialstyrelsen ønsker at vide, om Digitaliseringsstyrelsen oplyser den afsendende myndighed om hvilke konkrete data, metadata vedrører.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen har forstået spørgsmålet som, at Socialstyrelsen spørger, om der videregives CPR-numre til andre end modtageren og den pågældende offentlige afsender. Digitaliseringsstyrelsen kan oplyse at CPR-numre ikke udgør metadata, og at CPR-numre ikke videregives uden lovhjemmel.

3.7 Fortrolighed

Forsikring & Pension bemærker, at det afhængigt af omfanget og karakteren af personoplysninger, der er adgang til i løsningen, klart bør fremgå af bestemmelsen om fortrolighed i § 5, at Digitaliseringsstyrelsen på anmodning fra den dataansvarlige skal kunne dokumentere, at

de pågældende personer er underlagt ovennævnte tavshedspligt og underlagt instruktionsbeføjelse, samt gælde en særlig skærpet fortrolighed, ligesom det bør præciseres, at denne skal gælde tidsubegrænset.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen kan oplyse, at der vil blive udarbejdet dokumentation for den pålagte tavshedspligt og instruktion af medarbejdere med adgang til personoplysninger i Digital Post-løsningen.

3.8 Behandlingssikkerhed

Datatilsynet bemærker til udkastets § 6 og § 7, at det beskriver forhold omkring databehandlerens iagttagelse af den fornødne sikkerhed og autorisation. Datatilsynet anerkender, at udkastet indeholder flere elementer, af hvad der kan anses for passende tekniske og organisatoriske foranstaltninger til at iagttage databeskyttelsesforordningens krav i artikel 32, stk. 1. Det er dog Datatilsynets opfattelse, at udkastets tekst ikke kan stå alene for den enkelte dataansvarlige. Det vil således være nødvendigt for den dataansvarlige at have en beskrivelse af, hvordan de enkelte foranstaltninger konkret er løst på baggrund af den risikovurdering, der er forudsat udført efter udkastets § 6, stk. 1. Det står herudover ikke Datatilsynet klart, hvorledes udkastets § 6, stk. 4, og § 7 skal forstås i sammenhæng, da der tematisk er et overlap, der ikke forekommer stringent.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen tilpasser bestemmelserne i overensstemmelse med Datatilsynets bemærkninger, så det tydeligere fremgår, at foranstaltningerne fastsættes på baggrund af en risikovurdering. De dataansvarlige vil i øvrigt få adgang til en sammenfatning af denne på styrelsens hjemmeside. Endvidere præciseres det, at Digitaliseringsstyrelsen gennemfører passende tekniske og organisatoriske foranstaltninger, blandt andet logning af brug og adgang til personoplysninger. Derudover er der tilstræbt en klarere adskillelse af temaerne i § 6 og § 7.

Forsikring & Pension bemærker, at de mener, at der er behov for en præcisering af hvilke data, Digitaliseringsstyrelsen har adgang til, herunder om det alene er metadata genereret ved forsendelserne, eller om der også er adgang til data i selve de dokumenter, der sendes via løsningen. Forsikring & Pension bemærker, at sidstnævnte ikke burde være nødvendigt for håndtering af løsningen og derfor heller ikke muligt.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen er enige i, at det ikke bør være muligt for styrelsen at se indholdet af meddelelser i Digital Post. Som det fremgår af lovforslagets almindelige bemærkninger, er det alene borgere og virksomheder, der har råde- og ejendomsretten over deres egne meddelelser efter modtagelsen, og disse er kun tilgængelige for adressaten.

Forsvarsministeriets Personalestyrelse bemærker, at logning ikke nævnes eksplicit som en relevant foranstaltning i § 6, stk. 2, og spørger, om det dermed kan konkluderes, at der ikke logges. Styrelsen foreslår, at logning tilføjes som en del af § 6, stk. 2.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen er enige i bemærkningen og tilføjer den foreslåede foranstaltning om logning.

KL bemærker, at det fremgår af den foreslåede § 6, stk. 5, at "Den enkelte offentlige afsender er ansvarlig for at gennemføre egne relevante organisatoriske og tekniske sikkerhedsforanstaltninger, som knytter sig til den offentlige afsenders rolle som dataansvarlig i forbindelse med anvendelsen af Digital Post." Dette følger allerede af den foreslåede bestemmelse i § 2, stk. 4, hvorefter "Offentlige afsendere er ansvarlige for, at den behandling af personoplysninger, som finder sted i forbindelse med deres anvendelse af Digital Post, sker inden for rammerne af databeskyttelsesforordningen, databeskyttelsesloven og retshåndhævelsesloven." Bestemmelsen er ifølge KL overflødig og følger ikke af Datatilsynets standardkontraktbestemmelser. KL vil derfor anbefale, at § 6, stk. 5, udgår af bekendtgørelsesudkastet, særligt med henblik på at undgå, at kommunerne får opfattelsen af at blive pålagt yderligere krav som følge af bestemmelsen. Som konsekvens heraf bør § 10, stk. 3, nr. 1, hvor forpligtelsen gentages, efter KL's opfattelse også udgå.

Da § 6, stk. 6, om Digitaliseringsstyrelsens iagttagelse af reglerne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger ligeledes ikke følger af Datatilsynets standardkontraktbestemmelser, vil KL også anbefale, at denne bestemmelse udgår af udkastet. Både for at sikre den fornødne genkendelighed i forhold til Datatilsynets standardkontraktbestemmelser, men også da kravet efter KL's opfattelse følger umiddelbart af udkastets § 2, stk. 5: "Digitaliseringsstyrelsen og de dataansvarlige er hver især underlagt de opgaver og ansvar, der følger af databeskyttelsesforordningens generelle regler om den dataansvarlige og databehandleren (...)". Bestemmelsen er derfor ifølge KL overflødig i relation til bekendtgørelsesudkastet.

Digitaliseringsstyrelsens bemærkninger:

Efter Digitaliseringsstyrelsens opfattelse påhviler det den enkelte dataansvarlige at gennemføre egne relevante tekniske og organisatoriske sikkerhedsforanstaltninger, som knytter sig til den offentlige afsenders rolle som dataansvarlig i forbindelse med anvendelsen af Digital Post. Derfor kan Digitaliseringsstyrelsen ikke imødekomme ønsket om at lade § 6, stk. 5, og § 10, stk. 3, nr. 1, udgå.

I relation til forslaget om at lade § 6, stk. 6, udgå, er Digitaliseringsstyrelsen ikke enig i, at den er overflødig. Dette skyldes, at Digitaliseringsstyrelsen med indgåelsen af kontrakten for den nye Digital Post-løsning bliver dataansvarlig for selve it-systemet og dermed også for indretningen deraf og derved også databeskyttelse gennem design og standardindstillinger. Digitaliseringsstyrelsen finder det derfor hensigtsmæssigt at oplyse de dataansvarlige offentlige afsendere om, at ansvaret for dette påhviler styrelsen.

Region Midtjylland bemærker til bekendtgørelsens § 6, at denne efter regionens opfattelse bør stille eksplicit krav til, at Region Midtjylland/dataansvarlig får mulighed for at godkende Digitaliseringsstyrelsens risikovurdering, som Digitaliseringsstyrelsen efter bekendtgørelsen har ansvar for, jf. stk. 1, samt at det sikres, at regionen har mulighed for at få dokumentation for, at Digitaliseringsstyrelsen efterlever artikel 25. Region Midtjylland spørger endvidere, om databehandleren overhovedet kan tage ansvaret for tilsynet med underdatabehandlerne, jf. stk. 6.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen er enige i, at det er formålstjenligt at stille de oplysninger til rådighed for de dataansvarlige, der er nødvendige for, at de kan efterleve deres forpligtelser i relation til behandlingssikkerheden. Digitaliseringsstyrelsen kan oplyse, at styrelsen vil stille alle relevante og nødvendige oplysninger til rådighed for de dataansvarlige offentlige afsendere. Digitaliseringsstyrelsen kan endvidere oplyse, at der ikke gennemføres en godkendelsesproces i relation til risikovurderingen, men at de dataansvarlige offentlige afsendere gøres bekendt med indholdet, når en sammenfatning af den stilles til rådighed på styrelsens hjemmeside. Dertil bemærkes det, at eventuelle bemærkninger hertil kan rettes til styrelsen, som vil medtage disse i det løbende arbejde med behandlingssikkerheden.

Med hensyn til tilsynet med underdatabehandlere, er det Digitaliseringsstyrelsens opfattelse, at styrelsen er mest nærliggende til at føre dette tilsyn. Styrelsen vil stille dokumentationen for dette tilsyn til rådighed for de dataansvarlige.

Region Syddanmark bemærker til § 6, stk. 2, nr. 3, om ”Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af fysisk eller teknisk hændelse”, at regionen foreslår, at ”rettidigt” defineres som et konkret servicemål i en Service Level Agreement.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen bemærker, at det i kontrakten om den kommende Digital Post-løsning fremgår, at der udarbejdes en it-beredskabsplan, hvor det nærmere vil blive beskrevet og defineret, hvorledes it-beredskabet udmøntes i praksis, herunder målsætninger for at begrænse skadevirkningerne, understøtte en smidig overgang til alternative driftsfaciliteter, understøtte smidig retablering af data og systemer mv. De konkrete krav til retableringsmål fremgår af driftsaftalerne med leverandøren og vil blive beskrevet i it-beredskabsplanen.

3.9 Anvendelse af underdatabehandlere

Datatilsynet bemærker, at følgende om Digitaliseringsstyrelsens brug af underdatabehandler fremgår af udkastenes § 8, stk. 1: ”Digitaliseringsstyrelsen har generel godkendelse til at anvende underdatabehandlere til Digital Post. Planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere offentliggøres på Digitaliseringsstyrelsens hjemmeside.”

Det følger af databeskyttelsesforordningens artikel 28, stk. 2, at en databehandler ikke kan gøre brug af en anden databehandler uden forudgående specifik eller generel skriftlig godkendelse fra den dataansvarlige. Videre fremgår det af bestemmelsen i artikel 28, stk. 2, at i tilfælde, hvor der er givet en generel skriftlig godkendelse, skal databehandleren underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.

Datatilsynet skal på den baggrund henstille, at det kommer til at fremgå af § 8 i bekendtgørelserne, at den dataansvarlige har mulighed for at gøre indsigelser mod ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen indsætter en tilføjelse til § 8, stk. 1, hvorefter databehandleren skriftligt skal underrette den dataansvarlige 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).

Forsikring & Pension bemærker, at bekendtgørelsen efter Forsikring & Pensions opfattelse ikke indeholder en ret for den dataansvarlige til at godkende og gøre indsigelse mod Digitaliseringsstyrelsens underdatabehandlere, hvor Digitaliseringsstyrelsen er tillagt en ret til at vælge, samt udskifte disse uden krav om godkendelse eller forudgående høring af de dataansvarlige. Varsling om udskiftning af underdatabehandlere sker alene via Digitaliseringsstyrelsens hjemmeside, og uden tidsfrist. Der bør ifølge Forsikring & Pension fastsættes en varslingsfrist på minimum 1-2 måneder og med mulighed for at komme med begrundede indsigelser (høring).

Valgte underdatabehandlere fremgår alene på styrelsens hjemmeside. Det bør efter Forsikring & Pensions mening præciseres, hvor disse oplysninger kan findes på styrelsens hjemmeside, og der bør som minimum ske notifikation, hvis der sker ændringer i underdatabehandlerne.

Digitaliseringsstyrelsen bør ifølge Forsikring & Pension samtidig oplyse om brugen af underdatabehandlernes eventuelle underdatabehandlere.

Det bør ligeledes ifølge Forsikring & Pension fremgå af Digitaliseringsstyrelsens hjemmeside, hvor data opbevares (lokation).

Digitaliseringsstyrelsens tilsyn med deres underdatabehandlere sker blandt andet gennem fremsendelse af en årlig revisionserklæring fra en uafhængig revisor. Det bør efter Forsikring & Pensions mening klart fremgå, hvilken standard revisorerklæringen skal baseres på (f.eks. ISAE 3000 og/eller ISO 277001) og at den skal stilles til rådighed for de dataansvarlige.

Det bør endvidere, ifølge Forsikring & Pension, fremgå af bekendtgørelsen, at Digitaliseringsstyrelsen skal imødekomme de dataansvarliges begrundede rimelige krav om yderligere sikkerhedsforanstaltninger i forhold til underdatabehandlere, f.eks. som følge af konstateret databrud og sikkerhedsbrist hos underdatabehandleren, den fremsendte revisorerklæring, nye regler eller skærpet praksis mv.

Digitaliseringsstyrelsens bemærkninger:

Til forslaget om at indsætte en varslingsfrist for indsigelse henvises til besvarelsen af spørgsmålet lige ovenfor.

Med hensyn til offentliggørelse af brugen af underdatabehandlere kan det oplyses, at den konkrete leverandør ikke anvender underdatabehandlere. I det omfang der fremtidigt måtte blive behov for underleverandører, vil dette blive meldt ud til de dataansvarlige offentlige afsendere.

Digitaliseringsstyrelsen kan på Forsikring & Pensions ønske om, at det offentliggøres, hvor data opbevares, svare afkræftende på dette, da det af hensyn til statens sikkerhed og sikkerheden for Digital Post-løsningen ikke oplyses, hvor data opbevares henne. Det bemærkes, at data opbevares i Danmark i overensstemmelse med lokationskravet i databeskyttelseslovens § 3, stk. 9.

I relation til Forsikring & Pensions forslag om at stille krav til en specifik standard, revisorerklæringer skal baseres på, er det efter Digitaliseringsstyrelsens opfattelse hensigtsmæssigt at have mulighed for at tilpasse krav til revisorerklæringer over tid, da der forventes at ske udvikling på dette område, hvorfor der ikke defineres specifikke typer af revisorerklæringer i bekendtgørelserne.

Region Hovedstaden bemærker til § 8, stk. 3, at regionen bakker op om, at Digitaliseringsstyrelsen varetager en række opgaver i forhold til brugen af underdatabehandlere i Digital Post-løsningen, som typisk ellers varetages af den dataansvarlige. Regionen er dog usikker på, hvad konstruktionen betyder i praksis for regionens ansvar som dataansvarlig. Når opgaven med bekendtgørelsen overflyttes til Digitaliseringsstyrelsen, er der ifølge regionen behov for, at det præciseres, hvilket ansvar den enkelte region, eller anden offentlig afsender, fortsat har i forhold til underdatabehandlere.

Region Midtjylland bemærker til bekendtgørelsens § 8, at der efter regionens opfattelse bør sendes samlet orientering ud til alle dataansvarlige, når der tilføjes eller udskiftes en underdatabehandler, og de dataansvarlige skal have mulighed for at give tilbagemelding, hvis der er bemærkninger eller forhold, som de dataansvarlige normalt ikke ville acceptere.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen henviser til besvarelsen af spørgsmålene ovenfor.



Region Syddanmark anerkender, at det giver mening, at Digitaliseringsstyrelsen nu selv kan vælge ”underdatabehandlere” til Digital Post-løsningen, samt at Digitaliseringsstyrelsen selv er ansvarlig for, at deres ”underdatabehandlere” efterlever kravene i databeskyttelsesforordningen. Samtidigt finder regionen det dog bekymrende, at Digitaliseringsstyrelsens valg af hovedleverandør til Digital Post (Netcompany) har underafdelinger i tredjelande. Regionen opfordrer derfor Digitaliseringsstyrelsen til at være særligt opmærksom på dette forhold.

Regionen bemærker endvidere, at der i bekendtgørelsen er anvendt ordet ”underdatabehandleraftale”. Det bør efter regionens opfattelse erstattes med ”databehandleraftale”.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen kan oplyse, at opbevaringen af personoplysninger i Digital Post vil ske i Danmark i overensstemmelse med lokationskravet i medfør af databeskyttelseslovens § 3, stk. 9. Opbevaringen vil til enhver tid overholde de gældende databeskyttelsesretlige regler. Styrelsen er klar over, at Netcompany A/S har et datterselskab i Vietnam. Dette selskab behandler ikke personoplysninger fra Digital Post. Netcompanys vietnamesiske datterselskab har heller ikke derudover adgang til at tilgå personoplysninger i Digital Post-løsningen.

Digitaliseringsstyrelsen bemærker endvidere, at brugen af termen ”underdatabehandleraftale” tjener det formål, at bidrage til overskuelighed over konstruktionen ifm. beskrivelsen i bekendtgørelserne. Når termen underdatabehandler benyttes, henvises til Digitaliseringsstyrelsens indgåelse af databehandleraftaler med underleverandører.

Region Syddanmark bemærker til § 8, at regionen i udgangspunktet ikke anvender generel godkendelse af nye underdatabehandlere, men godt kan se behovet herfor i denne konstruktion. Imidlertid er offentliggørelse af nye underdatabehandlere på Digitaliseringsstyrelsens hjemmeside ifølge regionen ikke tilstrækkeligt til at opfylde databehandlerens forpligtelse til at underrette den dataansvarlige, jf. databeskyttelsesforordningens artikel 28, stk. 2. Regionen ser gerne, at det som minimum bliver muligt at tilmelde sig en ordning, hvor man får besked om, at der er sket ændringer af underdatabehandlere samt nogle minimumsoplysninger om denne underdatabehandler til vurdering af, om de kan accepteres, idet disse informationer er afgørende for, at regionen kan anvende sin ret til at gøre indsigelse mod ændringerne.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen henviser til det tidligere svar om underretning og indsigelsesret, hvorefter der er sket tilføjelse til bekendtgørelsesudkastenes § 8, stk. 1.

3.10 Overførsel til tredjelande eller internationale organisationer

Forsikring & Pension mener som udgangspunkt, at der kun bør ske overførsel af data til tredjelande efter dokumenteret instruks fra de dataansvarlige, der også er ansvarlige for at sikre, at der foreligger det nødvendige overførselsgrundlag ved overførsel af data til tredjelande. Forsikring & Pension bemærker videre, at det i den forbindelse vil være afgørende, at den dataansvarlig har kontrol over, at der ved transmission af meddelelser via tjenesten ikke

benyttes underdatabehandlere beliggende uden for EU/EØS, og som gør, at der sker tredjelandsoverførsel, hvilket ikke for nuværende vil kunne ske efter aftalen.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen kan bekræfte, at styrelsen ikke vil overføre personoplysninger til tredjelande, da Digital Post er omfattet af lokationskravet og derfor alene vil opbevare og behandle persondata inden for landets grænser. På den baggrund er der indsat et nyt § 9, stk. 1, der afspejler dette.

Det kan supplerende oplyses, at slutbrugernes adgang til Digital Post imidlertid ikke er begrænset til kun at kunne ske fra Danmark, og at styrelsen ikke kontrollerer, hvor borgere og virksomheder logger på fra. Der henvises endvidere til bemærkningerne ovenfor om brug af underdatabehandlere.

Hvis en dataansvarlig offentlig afsender eller juridisk enhed vil instruere Digitaliseringsstyrelsen i at sende digital post til tredjelande eller internationale organisationer vil det kræve en særskilt instruks, som det fremgår af § 9.

Sammenfattende kan det generelt bemærkes, at digital post kun kan afsendes af offentlige afsendere til modtagere med et dansk CPR- eller CVR-nummer, hvorfor overførsler til offentlige myndigheder eller internationale organisationer i tredjelande ikke er en del af formålet med anvendelsen af Digital Post, og at en offentlig afsender heller ikke har mulighed for at foretage en sådan forsendelse af en meddelelse via postløsningen.

KL ser et behov for, at Digitaliseringsstyrelsen i forhold til den del af reguleringen, der omhandler overførsler af data til tredjelande bidrager med at tilvejebringe det gyldige overførselsgrundlag. Den vurdering af tredjelandenes databeskyttelsesniveau, herunder tredjelandenes lovgivning, som er nødvendig for at sikre, at der foreligger et gyldigt overførselsgrundlag, når EU's standardkontraksbestemmelser anvendes, mener KL ikke, det er realistisk, at kommunerne pålægges alene.

Det fremgår nærmere af § 9, at "Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer kun [må] foretages af Digitaliseringsstyrelsen på baggrund af dokumenteret instruks herom fra den dataansvarlige offentlige afsender og altid [skal] ske i overensstemmelse med databeskyttelsesforordningens kapitel V (...) ". Instruksen fremgår imidlertid ikke af bekendtgørelsesudkastet. Af Datatilsynets standardkontraksbestemmelser fremgår instruksen i forhold til tredjelandsoverførsler imidlertid af bilag C, C.6. KL vil anbefale, at det kommer til at fremgå af bekendtgørelsen, hvorledes instruksen vedrørende tredjelandsoverførsler tænkes givet. KL hæfter sig i den forbindelse også ved, at der i § 9, stk. 3, er indføjet en bestemmelse, som ikke følger af Datatilsynets standardkontraksbestemmelser: "Ved overførsler omfattet af stk. 1, er den offentlige afsender ansvarlig for at sikre, at der foreligger et gyldigt overførselsgrundlag i henhold til databeskyttelsesforordningens kapitel V." KL vil opfordre til, at denne tilføjede bestemmelse ændres således, at ansvaret for et gyldigt overførselsgrundlag er Digitaliseringsstyrelsens i deres rolle som dataeksportør eller, at bestemmelsen eventuelt helt udgår af bekendtgørelsen. KL ser et væsentligt behov for, at

de udfordringer med at sikre gyldige overførselsgrundlag ved tredjelandsoverførsler som følge af Schrems II-dommen løftes af Digitaliseringsstyrelsen, da kommunerne ikke kan løfte denne opgave. Både at få indgået standardkontraktbestemmelser, jf. databeskyttelsesforordningens artikel 46, stk. 2, litra c, med relevante leverandører/underdatabehandlere men i særdeleshed at få udført de påkrævede vurderinger af databeskyttelsesniveauet i de relevante tredjelande samt udpeget relevante kompenserende foranstaltninger.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen har udformet bekendtgørelserne, så de opfylder kravene til at stå i stedet for en databehandlaftale. § 9 er derfor udformet for opfyldte disse krav. Digitaliseringsstyrelsen vil ikke af egen drift overføre personoplysninger til tredjelande eller internationale organisationer, hvorfor en eventuel overførsel vil kræve en specifik og entydig instruks fra den offentlige afsender samt dokumentation for, at der foreligger et gyldigt overførselsgrundlag iht. databeskyttelsesforordningens kapitel V. På den baggrund kan styrelsen oplyse, at det ikke kommer til at fremgå af bekendtgørelsen, hvorledes instruksen vedrørende tredjelandsoverførsler tænkes givet.

Digitaliseringsstyrelsen vil ikke ændre bestemmelserne, således at ansvaret for et gyldigt overførselsgrundlag pålægges Digitaliseringsstyrelsen i rollen som dataeksportør, da ansvaret for dette må henhøre til den pågældende offentlige afsender. Digitaliseringsstyrelsen vil endvidere ikke lade bestemmelsen udgå.

Sammenfattende kan det generelt bemærkes, at digital post kun kan afsendes af offentlige afsendere til modtagere med et dansk CPR- eller CVR-nummer, hvorfor overførsler til offentlige myndigheder eller internationale organisationer i tredjelande ikke er en del af formålet med anvendelsen af Digital Post, og at en offentlig afsender heller ikke har mulighed for at foretage en sådan forsendelse af en meddelelse via postløsningen.

Region Hovedstaden bemærker til § 9, stk. 3, at det fremgår, at det er den offentlige afsender, der skal sikre et tilstrækkeligt overførselsgrundlag i forhold til Databeskyttelsesforordningens kapitel V. Regionen mener ikke, at det vil være hensigtsmæssigt, hvis samtlige offentlige afsendere eksempelvis vil skulle indgå EU-standardkontrakter med en underleverandør i et tredjeland. Det vil efter regionens opfattelse være mere hensigtsmæssigt, hvis der i stedet laves en fælles model for dette, som de dataansvarlige skal godkende, eller hvis det skrives ind i bekendtgørelsen, at Digitaliseringsstyrelsen bistår den offentlige afsender med at sikre et overførselsgrundlag.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen kan oplyse, at der ikke vil blive antaget leverandører eller underleverandører i tredjelande til at varetage opgaver ifm. udvikling og drift af Digital Post-løsningen, og hvor der sker opbevaring af personoplysninger. Digitaliseringsstyrelsen har udformet bekendtgørelserne, så de opfylder kravene til at stå i stedet for en databehandlaftale. § 9 er derfor udformet for opfyldte disse krav. Digitaliseringsstyrelsen vil ikke af egen drift overføre

personoplysninger til tredjelande eller internationale organisationer. Der henvises til svaret ovenfor for en uddybning heraf.

Region Syddanmark bemærker, at Digital Post er omfattet af lokationskravet, jf. databeskyttelseslovens § 3, stk. 9, hvilket medfører en række skærpede krav til behandling af personoplysninger i denne løsning, herunder placering af data i Danmark mv.

Regionen bemærker endvidere, at bekendtgørelsens § 9 omhandler overførsel til tredjelande eller internationale organisationer, idet der henvises til databeskyttelsesforordningens kapitel 5 herom. Citat fra bekendtgørelsen: "Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af Digitaliseringsstyrelsen på baggrund af dokumenteret instruks herom fra den dataansvarlige offentlige afsender og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V," jf. udkastets § 9, stk. 1.

Imidlertid anser regionen ikke dette som tilstrækkeligt af følgende to grunde:

I) Databeskyttelsesloven, hvor databeskyttelsesforordningen hører under, er begrænset gennem § 1, stk. 3: "Regler om behandling af personoplysninger i anden lovgivning, som ligger inden for databeskyttelsesforordningens rammer for særregler om behandling af personoplysninger, går forud for reglerne i denne lov." En sådan lovgivning kan f.eks. være sundhedsloven (LBK nr 1286 af 02/11/2018), herunder § 49: "Sundhedsministeren fastsætter nærmere regler om videregivelse af oplysninger efter dette kapitel til tredjelande." Da væsentlige dele af datastrømme i den offentlige digitale post udspringer fra sundhedsvæsenet, er disse dele ikke alene underlagt databeskyttelsesloven, men også underkastet sundhedsloven.

II) Databeskyttelsesloven indeholder i § 3, stk. 9, det såkaldte lokationskrav (tidligere "krigsreglen"): "Justitsministeren kan efter forhandling med vedkommende minister fastsætte regler om, at personoplysninger, der behandles i nærmere bestemte it-systemer, og som føres for den offentlige forvaltning, helt eller delvis alene må opbevares her i landet." I vejledningen herom skrives eksplicit: "Som eksempler på it-systemer, der af justitsministeren allerede er blevet vurderet som omfattet af lokationskravet, kan Digitaliseringsstyrelsens it-systemer NemLog-in3, MitID samt Digital Post nævnes." (Vejledningens afsnit 3.6) Vejledningens eksempel pointerer, at såkaldte "leverandørsystemer" til Digital Post ikke omfattes af lokationskravet, men at "Det er således det pågældende it-system med de indeholdte personoplysninger, der omfattes af lokationskravet med det formål at sikre, at danske myndigheder har adgang til det pågældende it-system." Digitaliseringsstyrelsen er som databehandler derved underlagt lokationskravet.

På baggrund heraf er det ifølge regionen problematisk at forestille sig tilfælde, hvor databehandling, eventuelt ved underdatabehandlere, kan foregå i et tredjeland. Bekendtgørelsens § 9 bør tilpasses/tydeliggøres jf. dette.

Region Syddanmark gør opmærksom på, at ovenstående bemærkning gør sig gældende for begge § 9 i udkastene til bekendtgørelser.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen kan oplyse, at der ikke vil blive antaget leverandører eller underleverandører i tredjelande til at varetage opgaver ifm. udvikling og drift af Digital Post-løsningen, og hvor der sker opbevaring af personoplysninger. Se endvidere svarene ovenfor.

3.11 De registreredes rettigheder og sletning af personoplysninger

Region Hovedstaden bemærker, at da det er den dataansvarlige, som skal løfte oplysningspligten i forhold til de registrerede, vil det være en fordel, hvis de informationer Digitaliseringsstyrelsen i den forbindelse skal stille til rådighed for den dataansvarlige samles på ét sted, så der eksempelvis let kan linkes til dette fra den dataansvarliges persondatapolitik/privatlivspolitik.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen bemærker, at det kan synes fornuftigt at samle oplysningerne centralt og vil overveje at finde en hensigtsmæssig løsning, der kan imødekomme behovet herfor.

Region Midtjylland bemærker, at Digitaliseringsstyrelsen ikke sletter de i § 3 nævnte personoplysninger, som både indeholder almindelige personoplysninger, særlige kategorier af personoplysninger, personnumre og oplysninger om strafbare forhold, hvilket undrer Region Midtjylland. Digitaliseringsstyrelsen, skal som regionens databehandler, ifølge regionen, efter den dataansvarliges valg slette eller tilbagelevere alle personoplysninger til den dataansvarlige, efter at tjenesterne vedrørende behandling er ophørt, og skal slette eksisterende kopier, medmindre EU-retten eller medlemsstaten nationale ret foreskriver opbevaring af personoplysninger jf. databeskyttelsesforordningen artikel 28, stk. 3, litra g. Det vil efter regionens opfattelse sige, at Digitaliseringsstyrelsen ikke må behandle personoplysningerne, hvis det er uden for de dataansvarliges formål. Hvis Digitaliseringsstyrelsen ikke sletter personoplysningerne, når de dataansvarlige beder herom, og der ikke længere et formål med behandling af personoplysninger, vil Digitaliseringsstyrelsen handle uden for instruks fra de dataansvarlige og blive selvstændig dataansvarlig og skal derved selv sikre sig hjemmel til den videre behandling af personoplysningerne. Digitaliseringsstyrelsen gøres opmærksom herpå og anmodes af regionen om at redegøre for, hvorfor personoplysningerne ikke slettes.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen bemærker, som det fremgår af lovforslagets almindelige bemærkninger, jf. side 4 i lovforslag nr. L 47, folketingstidende 2020-2021, tillæg A, at det alene er borgere og virksomheder, der har råde- og ejendomsretten over deres egne meddelelser efter modtagelsen, og disse er kun tilgængelige for adressaten, som derfor er den, der kan beslutte om en meddelelse skal slettes, videresendes, gemmes mv. Digitaliseringsstyrelsen oplyser endvidere, at styrelsen fører hændelseslogs, der blandt andet kan dokumentere handlinger foretaget af brugerne i postløsningen. Formålet med disse er, at dokumentere om en given meddelelse er sendt, fremkommet mv. samt at fejlfinde og sikre it-løsningens sikkerhed. Selve

indholdet af meddelelserne fremgår ikke af disse logs. Slettefristen for disse hændelseslogs er under afklaring.

Region Midtjylland skal gøre opmærksom på, at de to bekendtgørelses § 12 ikke er enslydende. Region Midtjylland undrer sig over dette og beder Digitaliseringsstyrelsen forklare dette. Umiddelbart indstiller Region Midtjylland til, at § 12 i bekendtgørelse målrettet offentlige afsendere bliver enslydende § 12 i bekendtgørelse målrettet juridiske enheder. Vedrørende bekendtgørelses § 12, stk. 1, 2. pkt., bemærker regionen, at denne bemærkning kun er relevant, såfremt § 12 i bekendtgørelse målrettet offentlige afsendere ikke gøres enslydende eller lignende med § 12 i bekendtgørelse målrettet juridiske enheder.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen bemærker, at bekendtgørelsernes § 12 ikke kan justeres, så de bliver enslydende. Dette skyldes, at Digitaliseringsstyrelsen kun bliver databehandler for offentlige afsendere ved forsendelse af digital post. Digitaliseringsstyrelsen bliver derimod databehandler for såvel forsendelse som opbevaring for de juridiske enheder. For så vidt angår sletning, bemærker Digitaliseringsstyrelsen, at for borgere og virksomheder videreføres gældende ret, hvilket indebærer, at meddelelserne efter modtagelsen kun er tilgængelige for adressaten, der herefter har råderetten over meddelelserne. Det er derfor også adressaten, der kan beslutte om en meddelelse efterfølgende skal slettes, videresendes, gemmes, eksporteres mv. Derudover sletter Digitaliseringsstyrelsen hændelseslogs med passende intervaller, der pt. er under afklaring. Se i øvrigt svar ovenfor.

Region Nordjylland spørger, hvad hjemmelsgrundlaget og begrundelsen er for at oplysningerne som nævnt i § 3 ikke slettes. Hvordan hænger det sammen med bekendtgørelsen § 6, stk. 6, hvor det beskrives, at Digitaliseringsstyrelsen er ansvarlig for at leve op til databeskyttelsesforordningens artikel 25 om databeskyttelse gennem design og standardindstillinger, som blandt andet skal sikre effektiv implementering af databeskyttelsesprincipper så som dataminimering?

Region Syddanmark bemærker til § 12: Er begrundelsen for, at der ikke sker sletning af § 3-oplysninger, at den sletning alene kan ske af borgerne i deres indbakke? Såfremt dette ikke er tilfældet, skal der indsættes en slettefrist herfor.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen bemærker, som nævnt ovenfor, at det alene er borgeren eller virksomheden, der kan slette egne meddelelser i Digital Post-løsningen. Digitaliseringsstyrelsen oplyser endvidere, at styrelsen fører hændelseslogs, der blandt andet kan dokumentere handlinger foretaget af brugerne i postløsningen, hvilket også er nærmere beskrevet i svaret ovenfor.

3.12 Konsekvensanalyse

Forsikring & Pension bemærker, at det af § 10, stk. 3, nr. 4, i udkastet fremgår, at Digitaliseringsstyrelsen skal bistå med at foretage en konsekvensanalyse (DPIA). Forsikring & Pension



vil opfordre til, at myndighederne foretager en generel konsekvensanalyse, jf. databeskyttelsesforordningen artikel 35, stk. 10, og Datatilsynets vejledning om konsekvensanalyse, pkt. 5 om Fælles konsekvensanalyse, fremfor at de enkelte dataansvarlige hver især skal foretage en sådan. Dette bør ifølge Forsikring & Pension herefter afspejles i bekendtgørelsen.

Region Hovedstaden bemærker til § 10, stk. 3, at det fremgår af nr. 4, at Digitaliseringsstyrelsen skal bistå den dataansvarlige med ”forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse og 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.” Region Hovedstaden foreslår, at Digitaliseringsstyrelsen i stedet udarbejder én samlet generel konsekvensanalyse af Digital Post-løsningen i forhold til de overordnede kategorier af personoplysninger, løsningen behandler. Det vil være omkostningseffektivt både for de dataansvarlige og Digitaliseringsstyrelsen, som hermed ikke skal bistå alle de dataansvarlige aktører med at udarbejde hver deres konsekvensanalyse om den samme Digital Post-løsning.

Region Hovedstaden vurderer, at det er mest hensigtsmæssigt, at det er Digitaliseringsstyrelsen, der udarbejder en generel konsekvensanalyse, da Digitaliseringsstyrelsen varetager kontrakter og dialog med leverandører og underdatabehandlere i forhold til løsningen. Dette vil ifølge regionen også være i tråd med ansvarsfordelingen i § 6, hvor det fremgår, at Digitaliseringsstyrelsen iværksætter alle foranstaltninger, der kræves i henhold til databeskyttelsesforordningens artikel 32 om behandlingssikkerhed, mens de dataansvarlige aktører herimod ikke vil have reel mulighed for at mitigere eventuelle risici i løsningen, som en konsekvensanalyse identificerer. De dataansvarlige kan efter regionens mening efterfølgende eventuelt efter egen vurdering udarbejde supplerende konsekvensanalyser/risikovurderinger i forhold til deres konkrete anvendelse af Digital Post-løsningen, herunder data, som de sender via Digital Post, og som aktørerne derfor har ansvaret for. I forhold til hvordan dette kan gøres i praksis, vil Region Hovedstaden henlede opmærksomheden på, at artikel 35, stk. 10, i databeskyttelsesforordningen, giver mulighed for, at der i forbindelse med udarbejdelsen af lovforslag laves generelle konsekvensanalyser. En anden model er, at Digitaliseringsstyrelsen udarbejder en generel konsekvensanalyse, som stilles til rådighed for de aktører, som benytter løsningen i lighed med § 13, stk. 2, i bekendtgørelsen hvor Digitaliseringsstyrelsen stiller en tilsynsredegørelse til rådighed for aktørerne.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen kan oplyse, at styrelsen som dataansvarlig offentlig myndighed for Digital Post udarbejder en konsekvensanalyse vedrørende databeskyttelse i Digital Post-løsningen for at sikre, at behandlingen i postløsningen sker inden for rammerne af databeskyttelseslovgivningen. Digitaliseringsstyrelsen vil stille uddrag af konsekvensanalysen om Digital Post-løsningen til rådighed på styrelsens hjemmeside. Det er imidlertid styrelsens vurdering, at ikke alle dataansvarlige offentlige afsendere kan støtte deres behandling på denne konsekvensanalyse. De enkelte dataansvarlige offentlige afsendere bør overveje at udforme deres egne konsekvensanalyser, da de dataansvarlige offentlige afsendere f.eks. løbende kan tilpasse

egne tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre beskyttelsen af de registreredes rettigheder og frihedsrettigheder.

3.13 Underretning om brud på persondatasikkerhed til Datatilsynet

Forsikring & Pension bemærker, at det fremgår af udkastet, at underretning om et databrud bør ske uden unødigt ophold og ”om muligt” inden 48 timer efter at Digitaliseringsstyrelsen er blevet bekendt med bruddet. Det bør efter Forsikring & Pensions opfattelse præciseres, at dette ”skal ske” senest 48 timer efter, at Digitaliseringsstyrelsen er blevet bekendt med bruddet.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen tager bemærkningen til efterretning og tilretter bekendtgørelserne i overensstemmelse med forslaget, hvorefter ”om muligt” udgår.

Region Hovedstaden bemærker til § 11, stk. 2, at de vil foreslå, at Digitaliseringsstyrelsen underretter den dataansvarlige om eventuelle brud på persondatasikkerheden inden for 24 timer, så regionen som dataansvarlig har bedre mulighed for at risikovurdere bruddet og anmelde det til Datatilsynet, inden for de lovbestemte 72 timer. Regionen foreslår, at der eventuelt kan være tale om en foreløbig underretning således, at sagsbehandlingen hos den dataansvarlige kan påbegyndes inden alle forhold i forbindelse med bruddet nødvendigvis er fuldt afdækket.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen bemærker, at styrelsen vil underrette de dataansvarlige om brud på persondatasikkerheden uden unødigt forsinkelse og senest indenfor 48 timer efter, at styrelsen er blevet bekendt med bruddet, sådan at den dataansvarlige offentlige afsender kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til Datatilsynet. Dette betyder, at der i alle tilfælde vil ske underretning af de dataansvarlige hurtigst muligt. Digitaliseringsstyrelsen finder ikke anledning til at justere yderligere i bekendtgørelserne.

Region Hovedstaden bemærker til § 11, stk. 3, at det er en god praktisk løsning, at Digitaliseringsstyrelsen i visse situationer kan indberette et brud på vegne af de dataansvarlige. Det kan dog med fordel præciseres yderligere i hvilke situationer, henholdsvis § 11, stk. 2, og § 11, stk. 3, finder anvendelse, så der ikke opstår tvivl om ansvarsfordelingen i sagsbehandlingen af konkrete brud. Herudover er det vigtigt, at regionen som dataansvarlig underrettes, når Digitaliseringsstyrelsen indberetter et brud på vegne af de dataansvarlige. Dette bør fremgå af bekendtgørelsen.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen bemærker, at et større brud på persondatasikkerheden, der involverer et større antal dataansvarlige offentlige afsendere vil falde ind under § 11, stk. 3, jf. ordlyden af bestemmelsen, såfremt bruddet omfatter Digital Post-løsningen. Digitaliseringsstyrelsen



vil herefter foretage en samlet anmeldelse til Datatilsynet i overensstemmelse med databeskyttelsesforordningens artikel 33, stk. 1. Det vil blive uddybet i bekendtgørelsen, at Digitaliseringsstyrelsen underretter de dataansvarlige offentlige afsendere om bruddet. Et mindre brud på persondatasikkerheden, der f.eks. involverer en enkel dataansvarlig offentlig afsender vil falde ind under § 11, stk. 2.

Region Midtjylland bemærker til bekendtgørelsens § 11, stk. 2, at der står, at Digitaliseringsstyrelsens underretning om brud på persondatasikkerheden skal ske uden unødigt forsinkelse og om muligt senest inden for 48 timer, efter denne er blevet bekendt med bruddet. Selvom der er en mulighed for underretning senest inden for 48 timer, forudsætter Region Midtjylland, at Digitaliseringsstyrelsen uanset vil orientere hurtigst muligt.

Ligeledes er det Region Midtjyllands vurdering, at regionens frist for anmeldelse til Datatilsynet på 72 timer jf. databeskyttelsesforordningen artikel 33 først starter, når regionen som dataansvarlig bliver gjort bekendt med bruddet af Digitaliseringsstyrelsen. Region Midtjylland vurderer, at bekendtgørelsens § 11, stk. 3, er fornuftig, men regionen forudsætter, at regionen som dataansvarlig bliver underrettet om bruddet.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen bekræfter, at styrelsen vil underrette de dataansvarlige om brud på persondatasikkerheden uden unødigt forsinkelse og senest indenfor 48 timer efter, at styrelsen er blevet bekendt med bruddet, sådan at den dataansvarlige offentlige afsender kan overholde sin forpligtelse til inden for de efterfølgende 72 timer at anmelde bruddet på persondatasikkerheden til Datatilsynet.

Region Syddanmark bemærker til § 11, stk. 3, at der her gives adgang til, at Digitaliseringsstyrelsen må foretage en samlet anmeldelse til Datatilsynet ved brud på persondatasikkerheden. Det er lidt uklart for regionen, hvordan de enkelte dataansvarlige bliver informeret herom. Kan den samlede anmeldelse til Datatilsynet først ske efter, at bestemmelsens stk. 1 og 2, er opfyldt? Regionen vil gerne informeres inden, der sker anmeldelse til Datatilsynet, da der er en intern procedure, der skal aktiveres.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen bemærker, at bekendtgørelserne er tilpasset, således at Digitaliseringsstyrelsen underretter den dataansvarlige efter at være blevet opmærksom på et givent persondatasikkerhedsbrud, og inden der sendes en anmeldelse til Datatilsynet i medfør af bekendtgørelsens § 11, stk. 3.

Socialstyrelsen bemærker til § 11, stk. 3, at Digitaliseringsstyrelsen umiddelbart ikke kender indholdet af de fremsendte digitale breve og derved ikke på egen hånd har mulighed for at vurdere, om et eventuelt brud indebærer en risiko for den registreredes rettigheder eller frihedsrettigheder. Hvordan påtænker Digitaliseringsstyrelsen at foretage en sådan vurdering forud for eventuel indberetning til Datatilsynet?

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen er enige i Socialstyrelsens bemærkning, for så vidt angår indholdet af de digitale postmeddelelser. Digitaliseringsstyrelsen vil foretage en konkret vurdering af omfanget og størrelsen på persondatasikkerhedsbruddet, herunder hvorvidt der er flere dataansvarlige offentlige afsendere eller juridiske enheder inde over bruddet, og herefter underrettes de dataansvarlige om Digitaliseringsstyrelsens umiddelbare vurdering, førend der sendes en anmeldelse til Datatilsynet. Se gerne bemærkningen ovenfor.

3.14 Tilsyn og revision

Datatilsynet gør opmærksom på, at ordlyden af § 13, stk. 1, i udkastene bør ændres, således at det fremgår, at Digitaliseringsstyrelsen stiller alle oplysninger, der er relevante og nødvendige for at påvise overholdelse af kravene i bekendtgørelsen, til rådighed for de dataansvarlige, herunder oplysninger vedrørende underdatabehandlere, jf. § 8, stk. 6. Digitaliseringsstyrelsen lægger i § 13, stk. 3, i udkastene op til, at de dataansvarlige ikke har mulighed for at foretage inspektioner af Digitaliseringsstyrelsens fysiske faciliteter af ressourcemæssige og sikkerhedsmæssige grunde. Digitaliseringsstyrelsen udarbejder i stedet en årlig redegørelse for tilsyn med personoplysninger i Digital Post. Videre fremgår det af § 13, stk. 4, i udkastene, at Kontor for Revision og Tilsyn i Finansministeriets departement fører tilsyn med Digitaliseringsstyrelsen som databehandler på vegne af de dataansvarlige og udarbejder en tilsynsrapport på baggrund af deres tilsyn, der stilles til rådighed for de dataansvarlige. Datatilsynet har noteret sig, at Digitaliseringsstyrelsen har fundet det nødvendigt at afskære de dataansvarlige muligheden for at føre tilsyn med Digitaliseringsstyrelsens fysiske faciliteter af ressourcemæssige og sikkerhedsmæssige grunde. Datatilsynet har endvidere noteret sig, at der i udkastene lægges op til kompensatoriske foranstaltninger, blandt andet i form af Kontor for Revision og Tilsyn udøver tilsyn med Digitaliseringsstyrelsen på vegne af de dataansvarlige.

Det står ikke umiddelbart klart for Datatilsynet, om det er hensigten med udkastenes § 13, stk. 3, at alene muligheden for fysiske tilsyn hos Digitaliseringsstyrelsen afskæres, således at de dataansvarlige fortsat har mulighed for at foretage skriftlige tilsyn, eller om det i alle tilfælde vil være Kontor for Revision og Tilsyn, som skal føre tilsyn med Digitaliseringsstyrelsen på vegne af de dataansvarlige. Dette bør efter Datatilsynets opfattelse afklares i bekendtgørelserne. Efter Datatilsynets opfattelse er det endvidere vigtigt, at de dataansvarlige kan komme med anvisninger til Kontor for Revision og Tilsyns udøvelse af tilsynsbeføjelsen, blandt andet fordi særlige, individuelle forhold kan gøre sig gældende hos den enkelte dataansvarlige.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen kan bemærke i forhold til spørgsmålet om muligheden for, at de dataansvarlige kan føre skriftligt tilsyn, at det vil være muligt at anmode om supplerende oplysninger, såfremt en offentlig afsender har behov for uddybning. Dette vil blive præciseret i bekendtgørelsen. Et decideret skriftligt tilsyn vil imidlertid ikke kunne ske, blandt andet af hensyn til statens sikkerhed.

Som nævnt ovenfor vil Digitaliseringsstyrelsen stille alle relevante og nødvendige oplysninger til rådighed, hvilket vil blive præciseret i bekendtgørelsen. Dette forventes også at omfatte ofte stillede spørgsmål og svar. Det bemærkes endvidere, at de dataansvarliges muligheder for at give anvisninger og stille krav til tilsynet som udgangspunkt vil ske i regi af tilsynet, der foretages af Kontor for Revision og Tilsyn, hvilket vil blive nærmere meldt ud, når dette er endeligt afklaret.

Forsikring & Pension bemærker, at det er oplyst, at den dataansvarlige er afskåret fra at få adgang til at føre tilsyn på Digitaliseringsstyrelsens lokation af ressourcemæssige årsager. I stedet stilles der en revisorerklæring til rådighed fra uafhængig revisor. Det bør også her, ifølge Forsikring & Pension, præciseres, hvilken standard Digitaliseringsstyrelsens revisorerklæring skal baseres på (ISAE 3000 eller ISO 27701), hvor den stilles til rådighed og at dette skal ske vederlagsfrit. Digitaliseringsstyrelsen skal være ansvarlig for at implementere den dataansvarliges begrundede rimelige krav om supplerede sikkerhedsforanstaltninger, som revisorerklæringen eller andre oplysninger måtte give anledning til.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen vil som nævnt ovenfor stille alle relevante og nødvendige oplysninger til rådighed for de dataansvarlige offentlige afsendere på styrelsens hjemmeside. Dette forventes også at omfatte revisorerklæringerne, der dog kan være undtaget visse oplysninger af hensyn til disses karakter for at sikre statens sikkerhed mv.

Det kan bekræftes, at revisorerklæringerne udarbejdes efter anerkendte standarder, som udgangspunkt af typen ISAE 3000. Dette vil dog ikke blive præciseret i bekendtgørelsen, da der kan komme nye standarder, der viser sig bedre egnede til formålet. Alle typer erklæringer vil blive gjort tilgængelige for de dataansvarlige. Det vil komme til at fremgå af bekendtgørelserne, at revisorerklæringerne skal være i overensstemmelse med aktuelle standarder for GDPR-revisorerklæringer.

FSR – danske revisorer bemærker, at det mht. begge bekendtgørelser bør overvejes om man i § 13, stk. 4, skulle præcisere, at der er tale om en årlig handling.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen er enige i betragtningen og vil præcisere ordlyden i § 13, stk. 4, i overensstemmelse hermed.

Region Midtjylland spørger, om Datatilsynet mener, at dette er tilstrækkeligt til, at de dataansvarlige kan overholde sine forpligtelser efter databeskyttelsesforordningen, navnlig artikel 28, stk. 3, litra h?

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen forstår regionens spørgsmål, således, at der spørges til om styrelsen efter artikel 28, stk. 3, litra h, ”stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i denne artikel, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.” Datatilsynet bemærker, at ordlyden af § 13, stk. 1, i udkastene bør ændres, således at det fremgår, at ”Digitaliseringsstyrelsen stiller alle oplysninger, der er relevante og nødvendige for at påvise overholdelse af kravene i bekendtgørelsen, til rådighed for de dataansvarlige, herunder oplysninger vedrørende underdatabehandlere, jf. § 8, stk. 6.”

I den forbindelse bemærker Digitaliseringsstyrelsen, at det som nævnt ovenfor er formålstjenligt at stille de oplysninger til rådighed for de dataansvarlige, der er nødvendige for, at de kan efterleve deres forpligtelser i relation til behandlingssikkerheden. Digitaliseringsstyrelsen kan oplyse, at styrelsen vil stille alle relevante og nødvendige oplysninger til rådighed for de dataansvarlige offentlige afsendere.

Digitaliseringsstyrelsen bemærker for så vidt angår inspektioner, at de dataansvarlige ikke har mulighed for at foretage inspektioner af Digitaliseringsstyrelsens fysiske faciliteter af ressourcemæssige og sikkerhedsmæssige grunde. Digitaliseringsstyrelsen har valgt denne model, fordi fysisk inspektion, der skal udføres af alle dataansvarlige offentlige afsendere og juridiske enheder, vil medføre et uforholdsmæssigt ressourceforbrug for Digitaliseringsstyrelsen. Endvidere har Digitaliseringsstyrelsen af sikkerhedsmæssige grunde fravalgt at give mulighed for fysisk inspektion, da de oplysninger, de dataansvarlige efterspørger, kan være af fortrolig karakter. Det vil alene være ansatte i styrelsen og relevante databehandlere, der er sikkerhedsgodkendt, som vil have adgang til de af it-systemets oplysninger, der er relevante for administration af løsningen. Ydermere er Digital Post omfattet af lokationskravet i databeskyttelseslovens § 3, stk. 9, hvilket indebærer, at personoplysninger, der behandles i det pågældende it-system, opbevares inden for landets grænser af hensyn til statens sikkerhed. Digitaliseringsstyrelsen har derfor af disse grunde fravalgt at tillade fysiske inspektioner for at opnå sikker administration af de i it-systemet indeholdte personoplysninger.

Digitaliseringsstyrelsen udarbejder derfor i medfør af § 13, stk. 3, 2. pkt., i stedet en redegørelse om databehandlingen. Digitaliseringsstyrelsen vil stille redegørelsen til rådighed for de dataansvarlige offentlige afsendere på Digitaliseringsstyrelsens hjemmeside.

Region Syddanmark bemærker til § 13, at det her er anført, at informationer vedr. tilsyn stilles til rådighed for de dataansvarlige. Her savner regionen en mere konkret beskrivelse af, hvor disse oplysninger stilles til rådighed. Sker det eksempelvis via Digitaliseringsstyrelsens hjemmeside eller via en portal? Det er også et ønske fra regionens side, at der oplyses nogle relevante datoer eller at regionen modtager påmindelser ved nyt materiale. Dette skal ses i forhold til regionens planlægning.

Det er uklart for regionen, hvad redegørelsen efter § 13, stk. 2, vil indeholde i forhold til opfølgning på tilsyn med underdatabehandlere, herunder handlingsplaner ved eventuelle anmærkninger i revisorerklæringer.

Regionen har fuld forståelse for behovet for bestemmelsen i § 13, stk. 3, men mener, at der er brug for undtagelser hertil. Eksempelvis tungvejende forhold.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen bemærker til § 13, stk. 1, at styrelsen vil stille alle relevante og nødvendige oplysninger til rådighed for de dataansvarlige offentlige afsendere på styrelsens hjemmeside. Tilsvarende er regionens ønsker om at få oplyst datoer eller påmindelser af hensyn til regionens planlægning en del af det videre arbejde med forvaltningen.

Vedrørende spørgsmålet til § 13, stk. 2, oplyser styrelsen, at den konkrete tilsynsmodel er under nærmere afklaring, og at oplysningerne om tilsynet ville blive stillet til rådighed for de dataansvarlige i forbindelse med idriftsættelsen af postløsningen.

Digitaliseringsstyrelsen kan i relation til § 13, stk. 3, om inspektion endvidere oplyse, at styrelsen i stedet udarbejder redegørelse om databehandlingen. Digitaliseringsstyrelsen vil stille redegørelsen til rådighed for de dataansvarlige offentlige afsendere. Der henvises til svaret ovenfor for uddybning heraf.

Socialstyrelsen bemærker til § 13, stk. 4, at Finansministeriets tilsyn med Statens IT bliver fremlagt på blandt andet DPO hub-møde i regi af Statens IT. Rigsrevisionen har i den forbindelse tilkendegivet, at der ved denne fremlæggelse er sket behørig opfølgning på tilsynet ved deltagelse på disse møder. Socialstyrelsen spørger, hvordan Digitaliseringsstyrelsen påtænker at sikre opfølgningen på tilsyn, og hvordan den dataansvarlige påtænker at dokumentere, at opfølgningen har fundet sted.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen har noteret sig Socialstyrelsens bemærkning om, at Finansministeriets tilsyn med Statens IT bliver fremlagt på blandt andet DPO hub-møde i regi af Statens IT, samt at Rigsrevisionen anser, at der er sket behørig opfølgning på tilsynet ved en fremlæggelse på disse møder. Digitaliseringsstyrelsen bemærker i den forbindelse, at forslaget ikke imødekommes.

3.15 Offentlige afsendere

Forsikring & Pension ønsker at gøre opmærksom på, at forsikringsbranchens kommunikation med kunderne ofte har en karakter, hvor det er svært at se grunden til, at den ikke ligestilles med kommunikation fra det offentlige. En del af kommunikationen er således lovbunden f.eks. som følge af forsikringsaftaleloven. Forsikring & Pension spørger til mulighederne for se på, om denne kommunikation også kan smidiggøres.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen bemærker, at private virksomheders mulighed for at benytte den nye Digital Post-løsning som offentlige afsendere i deres kommunikation med kunder mv. falder uden for lov om Digital Post fra offentlige afsenders anvendelsesområde. Desuden vil en sådan anvendelse skulle vurderes efter reglerne om konkurrenceret og statsstøtte samt under hensyntagen til Digitaliseringsstyrelsens forpligtelse til at administrere sin kontrakt med leverandøren i overensstemmelse med de udbudsretlige regler.

For at åbne mulighed for at også private virksomheder kan kommunikere med borgerne inden for Digital Post-infrastrukturen, skaber seneste ændringslov nr. 1941 af 15. december 2020 til lov om Digital Post fra offentlige afsendere og bekendtgørelse nr. 2011 af samme dato om godkendelse af visningsklienter til Digital Post samt kompensation for forpligtelser til offentlig tjeneste for udbydere af kommercielle visningsklienter det retlige grundlag for, at der kan etableres kommercielle visningsklienter. Disse kan tilmed ansøge om økonomisk kompensation, hvis de udbyder supplerende ydelser, f.eks. giver borgerne mulighed for at modtage post fra både offentlige og private afsendere i samme postkasse. Denne tilskyndelse har blandt andet til formål at imødekomme virksomheders behov for at kommunikere med borgerne i en kontekst, som borgerne er vant til fra den nuværende leverandørs løsning. Der henvises endvidere til lovbemærkningerne til det tidligere fremsatte lovforslag nr. L 47, folketingstidende 2020-2021, tillæg A.

Region Midtjylland beder Digitaliseringsstyrelsen give en tilbagemelding på, om begge bekendtgørelser, der er i høring, er gældende for offentlige myndigheder?

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen kan oplyse, at styrelsen har udarbejdet to bekendtgørelser til henholdsvis offentlige afsendere og juridiske enheder for at gøre det klart, hvilken form for databehandling styrelsen foretager sig i forhold til de to forskellige dataansvarlige. Digitaliseringsstyrelsen kan derfor bekræfte, at det udelukkende er bekendtgørelsen om offentlige afsendere, som de offentlige myndigheder i kraft af deres tilslutning som offentlige afsendere i postløsningen, skal henholde sig til.

Det beror på en konkret vurdering, om en myndighed, en offentlig institution mv., er omfattet af begrebet ”offentlig afsender”. Såfremt en myndighed, en offentlig institution mv. falder ind under definitionen af offentlige afsendere efter Digital Post-loven og bekendtgørelsen om offentlige afsendere, men ikke var optaget i bilagene til bekendtgørelse om offentlige afsendere på tidspunktet for udbuddet af kontrakt om udvikling, drift, vedligeholdelse, support og videreudvikling af Digital Post, beror det endvidere på en udbudsretlig vurdering, hvorvidt dette er muligt.

Digitaliseringsstyrelsen kan endvidere oplyse, at hvis man ikke anses som offentlig afsender, anses man som juridisk enhed og omfattes dermed af bekendtgørelsen herom i forhold til dataansvaret i postløsningen. Man vil dermed som dataansvarlig i alle tilfælde være omfattet af den ene eller den anden bekendtgørelse.

Se tillige afsnit 3.16 nedenfor om tilpasningen af bekendtgørelsen for de offentlige afsenders databehandling for de retshåndhævende myndigheder.

3.16 Retshåndhævende myndigheder

Domstolsstyrelsen bemærker, at udkastene til bekendtgørelserne mangler en stillingtagen til behandling af personoplysninger omfattet af lov om retshåndhævende myndigheders behandling af personoplysninger (lov nr. 410 af 27. april 2017, retshåndhævelsesloven). Bekendtgørelserne vil derfor ikke finde anvendelse for behandling af personoplysninger, som domstolene foretager i sager med henblik på at retsforfølge strafbare handlinger, og som foretages med Digital Post.

Domstolsstyrelsen vil derfor foreslå, at der udarbejdes en tredje bekendtgørelse, som finder anvendelse for domstolenes og Procesbevillingsnævnets behandling af personoplysninger. Domstolsstyrelsen vil endvidere foreslå, at Digitaliseringsstyrelsen afklarer med de øvrige retshåndhævende myndigheder, om en sådan tredje bekendtgørelse skal omfatte de øvrige retshåndhævende myndigheders behandling af personoplysninger i Digital Post. Endelig vil Domstolsstyrelsen foreslå, at henvisningen til retshåndhævelsesloven fjernes fra § 2, stk. 4 i udkastet til de to bekendtgørelser.

Forsvarsministeriet og Forsvarsministeriets Auditørkorps kan tilslutte sig Domstolsstyrelsens høringssvar.

Digitaliseringsstyrelsens bemærkninger:

Digitaliseringsstyrelsen bemærker, at styrelsen i medfør af lovforslag nr. L 47, folketingsstidende 2020-2021, tillæg A, og de specielle bemærkninger til den foreslåede § 2 a (på side 15), har hjemmel til at fastsætte vilkår for Digitaliseringsstyrelsens behandling af personoplysninger for de retshåndhævende myndigheder i Digital Post-løsningen.

Digitaliseringsstyrelsen vil foretage tilpasning af den eksisterende bekendtgørelse for offentlige afsendere, således at det klart fremgår, at også de retshåndhævende myndigheder vil være omfattet af bekendtgørelsen.