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

I medfør af § 2 a, stk. 5, jf. stk. 3, i lov om Digital Post fra offentlige afsendere, jf. lovbekendtgørelse nr. 801 af 13. juni 2016, som ændret ved § 29 i lov nr. 503 af 23. maj 2018 og ved § 1 i lov nr. XX af dd. mm. 2021, fastsættes:

Anvendelsesområde

§ 1. Denne bekendtgørelse er udarbejdet af Digitaliseringsstyrelsen under henvisning til databeskyttelsesforordningens artikel 28 om forholdet mellem aktører, der har en rolle som henholdsvis dataansvarlig og databehandler i relation til behandling af personoplysninger i Digital Post.

Stk. 2. Efter databeskyttelsesforordningens artikel 28, stk. 3, skal en databehandlers behandling af personoplysninger være reguleret af en kontrakt eller andet retligt bindende dokument i henhold til EU-retten eller medlemslandenes nationale ret, der er bindende for databehandleren med hensyn til den dataansvarlige. Bekendtgørelsen er det retligt bindende dokument i medfør af databeskyttelsesforordningens artikel 28, stk. 3, som regulerer Digitaliseringsstyrelsens behandling af personoplysninger i Digital Post på vegne af den dataansvarlige, jf. § 2.

Dataansvarlig og databehandler

§ 2. Digitaliseringsstyrelsen stiller Digital Post til rådighed for forsendelse af meddelelser fra offentlige afsendere samt ved advisering af modtagerne via sms og e-mail ved levering af nye meddelelser samt ved fremsendelse af servicebeskeder fra offentlige afsendere via NemSMS, jf. § 2 a, stk. 5, jf. stk. 3, i lov om Digital Post fra offentlige afsendere.

Stk. 2. Offentlige afsendere er dataansvarlige for behandlingen af de personoplysninger, der er indeholdt i og metadata tilknyttet meddelelser og advisering heraf via sms og e-mail samt ved servicebeskeder via NemSMS, de sender via Digital Post.

Stk. 3. Digitaliseringsstyrelsen er databehandler for de offentlige afsendere, når disse sender meddelelser via Digital Post.

Stk. 4. 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.

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, navnlig artikel 28, for så vidt angår Digitaliseringsstyrelsen som databehandler, med de præciseringer, der følger af denne bekendtgørelse.

§ 3. Digitaliseringsstyrelsens behandling kan blandt andet omfatte følgende typer af personoplysninger:

1) Almindelige personoplysninger.
2) Særlige kategorier af personoplysninger (følsomme personoplysninger), i medfør af artikel 9, stk. 1 i databeskyttelsesforordningen.
3) Personnumre.
4) Oplysninger om strafbare forhold.

Stk. 2. Digitaliseringsstyrelsens behandling vedrører flere typer af registrerede personer, blandt andet borgere og medarbejdere. Oplysninger om de registrerede personer fremgår af indholdet i og metadata tilknyttet de meddelelser, som de offentlige afsendere sender via Digital Post.

Databehandleren handler efter instruks

§ 4. Digitaliseringsstyrelsens behandling af personoplysninger består i transmission og levering af meddelelser med tilknyttede metadata sendt via Digital Post til de af de offentlige afsendere anførte modtagere, samt ved advisering af modtagerne via sms og e-mail ved levering af nye meddelelser og ved fremsendelse af servicebeskeder fra offentlige afsendere via NemSMS. Digitaliseringsstyrelsens behandling af personoplysninger på vegne af de offentlige afsendere ophører således ved leveringen af meddelelserne til de af de offentlige afsendere anførte modtageres digitale postkasser samt ved leveringen af sms og e-mail advisering og ved fremsendelse af servicebeskeder fra offentlige afsendere via NemSMS.

Stk. 2. 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.

Stk. 3. Digitaliseringsstyrelsens behandling af personoplysninger i Digital Post på vegne af de offentlige afsendere er ikke tidsbegrænset, men varer indtil bekendtgørelsen ophæves.

Stk. 4. Digitaliseringsstyrelsen kan videregive metadata fra Digital Post til brug for udførelse af f.eks. statistiske eller videnskabelige undersøgelser, jf. databeskyttelseslovens § 10, når den rekvirerende aktør efter lovgivningen har hjemmel og de fornødne tilladelser til, at videregivelse af personoplysninger til sådanne formål kan ske.

Stk. 5. I forbindelse med videregivelser i henhold til stk. 4, bliver Digitaliseringsstyrelsen selvstændig dataansvarlig for de videregivne personoplysninger, og Digitaliseringsstyrelsen er ansvarlig for at sikre, at der er en gyldig hjemmel til videregivelsen.

Fortrolighed

§ 5. Digitaliseringsstyrelsen skal som databehandler sikre, at de personer, der er autoriseret til at behandle personoplysninger på vegne af de offentlige afsendere har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

Behandlingssikkerhed

§ 6. Digitaliseringsstyrelsen iværksætter alle foranstaltninger, der kræves i henhold til databeskyttelsesforordningens artikel 32 om behandlingssikkerhed. Digitaliseringsstyrelsen sikrer

herved, at der under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

Stk. 2. På baggrund af resultatet af den risikovurdering, som Digitaliseringsstyrelsen har gennemført, jf. § 6, stk. 1, gennemfører Digitaliseringsstyrelsen passende foranstaltninger for at imødegå de identificerede risici. Der kan alt efter, hvad der er relevant, være tale om følgende foranstaltninger:

1) Kryptering af personoplysninger.
2) Evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og tjenester.
3) Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af fysisk eller teknisk hændelse.
4) En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

Stk. 3. Digitaliseringsstyrelsen træffer de fornødne tekniske og organisatoriske foranstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med formålet for databehandlingen, der udføres af Digitaliseringsstyrelsen.

Stk. 4. Digitaliseringsstyrelsen fastsætter nærmere interne bestemmelser, i eget informationssikkerhedsledelsessystem, om sikkerhedsforanstaltninger i databehandlingen, der navnlig skal omfatte organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer. Der skal endvidere fastsættes instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af it-udstyr. Desuden skal der fastsættes retningslinjer for tilsynet med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for databehandlingen.

1) De interne bestemmelser gennemgås mindst én gang hvert år med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold hos Digitaliseringsstyrelsen.
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 stk. 4.
3) På steder, hvor der foretages behandling af personoplysninger, træffes der forholdsregler med henblik på at forhindre uvedkommendes adgang til oplysningerne.

Stk. 5. 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.

Stk. 6. Digitaliseringsstyrelsen er ansvarlig for iagttagelse af reglen om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i databeskyttelsesforordningens artikel 25 i forhold til udvikling, drift, vedligeholdelse og forvaltning af Digital Post.

Autorisation og adgangskontrol

§ 7. Kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles.

Stk. 2. Der må kun autoriseres personer, der beskæftiger sig med de formål, hvortil personoplysningerne behandles. De enkelte personer må ikke autoriseres til anvendelser, som de ikke har behov for.

Stk. 3. Der må endvidere autoriseres personer, for hvem adgang til oplysninger er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.

Stk. 4. Der træffes foranstaltninger for at sikre, at kun autoriserede personer kan få adgang, og at disse kun kan få adgang til de personoplysninger og anvendelser, som de er autoriserede til.

Stk. 5. Autorisationer, jf. stk. 1, skal angive, i hvilket omfang brugeren må forespørge, eksportere, indføre eller slette personoplysninger.

Stk. 6. Det skal sikres, at de autoriserede personer fortsat opfylder betingelserne i stk. 1-4.

Stk. 7. Kontrol i medfør af stk. 6 skal foretages mindst én gang hvert halve år.

Anvendelse af underdatabehandlere

§ 8. Digitaliseringsstyrelsen har generel godkendelse til at anvende underdatabehandlere til Digital Post. Planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere offentliggøres på Digitaliseringsstyrelsens hjemmeside.

Stk. 2. Ved anvendelse af underdatabehandlere er Digitaliseringsstyrelsen ansvarlig for at efterleve kravene i databeskyttelsesforordningens artikel 28. Digitaliseringsstyrelsen er herefter blandt andet forpligtet til:

1) Alene at anvende underdatadatabehandlere, der kan stille de fornødne garantier for, at de gennemfører de passende tekniske og organisatoriske sikkerhedsforanstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.
2) At sikre at der foreligger en gyldig underdatabehandleraftale mellem Digitaliseringsstyrelsen og en eventuel underdatabehandler.

Stk. 3. Digitaliseringsstyrelsens underdatabehandlere for Digital Post vil fremgå af Digitaliseringsstyrelsens hjemmeside. Oplysninger om underdatabehandlere kan fremsendes til de offentlige afsendere efter skriftlig anmodning herom til Digitaliseringsstyrelsen.

Stk. 4. Digitaliseringsstyrelsen sørger for at pålægge underdatabehandlere de samme databeskyttelsesforpligtelser, som dem, der er fastsat ved denne bekendtgørelse, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de passende tekniske

og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen.

Stk. 5. Digitaliseringsstyrelsen er således ansvarlig for – igennem indgåelsen af en underdatabehandleraftale – at pålægge en eventuel underdatabehandler mindst de forpligtelser, som Digitaliseringsstyrelsen selv er underlagt efter databeskyttelsesreglerne og denne bekendtgørelse.

Stk. 6. Digitaliseringsstyrelsen fører tilsyn med underdatabehandlerens overholdelse af underdatabehandleraftalen. De dataansvarlige har ikke mulighed for at føre tilsyn direkte med underdatabehandleren uden Digitaliseringsstyrelsens forudgående skriftlige godkendelse. De dataansvarlige får, til brug for eget tilsyn, mulighed for at modtage relevante informationer, som Digitaliseringsstyrelsen gennem tilsynet med underdatabehandleren, stiller til rådighed, jf. § 13, stk. 2. Tilsynet med underdatabehandlere udføres blandt andet ved at:

1) Underdatabehandleren én gang årligt skal indhente en revisionserklæring 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 revisionserklæringen fra underdatabehandleren, hvorefter den stilles til rådighed for de dataansvarlige offentlige afsendere.
2) Digitaliseringsstyrelsen, eller en uafhængig revisor bemyndiget af Digitaliseringsstyrelsen, har ret til at foretage inspektioner af underdatabehandlerens fysiske faciliteter, hvor der behandles personoplysninger samt modtage de nødvendige informationer til udførelsen af undersøgelsen af, hvorvidt underdatabehandleren har truffet de sikkerhedsforanstaltninger, der følger af underdatabehandleraftalen samt gældende databeskyttelsesret.
3) Digitaliseringsstyrelsen har løbende mulighed for at indhente informationer baseret på resultaterne af enten revisionserklæringen, inspektionen af de fysiske faciliteter eller de modtagende informationer. Når der er behov for det, er Digitaliseringsstyrelsen berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og denne bekendtgørelse.
4) Underdatabehandleren skal give myndigheder, eller deres udpegede repræsentanter, der efter EU-retten eller lovgivningen i en medlemsstat har ret til adgang til Digitaliseringsstyrelsens og underdatabehandlerens faciliteter, adgang til underdatabehandlerens fysiske faciliteter mod forevisning af behørig legitimation.

Stk. 7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver Digitaliseringsstyrelsen fuldt ansvarlig over for de dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.

Overførsel til tredjelande eller internationale organisationer

§ 9. 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. Uden dokumenteret instruks fra den dataansvarlige offentlige afsender kan Digitaliseringsstyrelsen således ikke inden for rammerne af denne bekendtgørelse:

1) Overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation.
2) Overlade behandling af personoplysninger til en underdatabehandler i et tredjeland.
3) Behandle personoplysningerne i et tredjeland.

Stk. 2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som Digitaliseringsstyrelsen ikke er blevet instrueret i at foretage af den dataansvarlige offentlige afsender, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Digitaliseringsstyrelsen er underlagt, skal Digitaliseringsstyrelsen underrette den dataansvarlige offentlige afsender om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

Stk. 3. 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.

Bistand til den dataansvarlige

§ 10. Digitaliseringsstyrelsen bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den offentlige afsenders forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder, som er fastlagt i databeskyttelsesforordningens kapitel III.

Stk. 2. Dette indebærer, at Digitaliseringsstyrelsen så vidt muligt skal bistå den offentlige afsender i forbindelse med, at den offentlige afsender i dens rolle som dataansvarlig skal sikre overholdelsen af nedenstående regler i databeskyttelsesforordningen:

1) Oplysningspligten ved indsamling af personoplysninger hos den registrerede, jf. artikel 13.
2) Oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede, jf. artikel 14.
3) Den registreredes indsigtsret, jf. artikel 15.
4) Retten til berigtigelse, jf. artikel 16.
5) Retten til sletning (»retten til at blive glemt«), jf. artikel 17.
6) Retten til begrænsning af behandling, jf. artikel 18.
7) Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling, jf. artikel 19.
8) Retten til indsigelse, jf. artikel 21.

Stk. 3. Digitaliseringsstyrelsen bistår den dataansvarlige med at sikre overholdelse af den offentlige afsenders forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Digitaliseringsstyrelsen som databehandler, jf. databeskyttelsesforordningens artikel 28, stk. 3, litra f. Dette indebærer, at Digitaliseringsstyrelsen under hensynstagen til behandlingens karakter skal bistå den enkelte offentlige afsender i forbindelse med, at denne skal sikre overholdelsen af:

1) Forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen, jf. § 6.
2) Forpligtelsen til at anmelde brud på persondatasikkerheden til Datatilsynet uden unødig forsinkelse og om muligt senest 72 timer, efter at den enkelte dataansvarlige er blevet bekendt

med bruddet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, jf. § 11.

3) Forpligtelsen til uden unødig forsinkelse at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, jf. § 11.
4) Forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, og forpligtelsen til at høre Datatilsynet inden behandling, hvis en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den enkelte dataansvarlige for at begrænse risikoen.

Underretning om brud på persondatasikkerhed til Datatilsynet

§ 11. Digitaliseringsstyrelsen underretter uden unødig forsinkelse den dataansvarlige offentlige afsender efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

Stk. 2. Digitaliseringsstyrelsens underretning til den dataansvarlige offentlige afsender skal ske uden unødig forsinkelse og om muligt senest indenfor 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. Den offentlige afsender underretter de registrerede om bruddet på persondatasikkerheden i overensstemmelse med kravene herom i databeskyttelsesforordningens artikel 34.

Stk. 3. Digitaliseringsstyrelsen kan på vegne af samtlige dataansvarlige offentlige afsendere omfattet af denne bekendtgørelse, under hensyn til sagens karakter, bruddets omfang og såfremt bruddet omfatter Digital Post-løsningen, foretage en samlet anmeldelse til Datatilsynet i overensstemmelse med databeskyttelsesforordningens artikel 33, stk. 1.

Stk. 4. I overensstemmelse med stk. 1 skal Digitaliseringsstyrelsen bistå den offentlige afsender med at foretage anmeldelse af bruddet til Datatilsynet. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som i medfør af databeskyttelsesforordningens artikel 33, stk. 3, skal fremgå af den dataansvarlige offentlige afsenders anmeldelse af bruddet til Datatilsynet:

1) Karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger.
2) De sandsynlige konsekvenser af bruddet på persondatasikkerheden.
3) De foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

Sletning af personoplysninger

§ 12. Digitaliseringsstyrelsens databehandling i medfør af denne bekendtgørelse ophører med levering af meddelelserne og ved leveringen af sms, e-mail advisering og servicebeskeder fra offentlige afsendere

via NemSMS til de anførte modtagere, jf. § 4, stk. 1. Digitaliseringsstyrelsen sletter ikke de i § 3 nævnte personoplysninger.

Tilsyn og revision

§ 13. Digitaliseringsstyrelsen stiller oplysninger, der er relevante og nødvendige for at påvise overholdelse af kravene i bekendtgørelsen, til rådighed for de dataansvarlige offentlige afsendere, herunder oplysninger vedrørende underdatabehandlere, jf. § 8, stk. 6.

Stk. 2. Digitaliseringsstyrelsen udarbejder årligt en redegørelse for tilsyn med personoplysninger i Digital Post. Redegørelsen udarbejdes på baggrund af denne bekendtgørelses §§ 6-11. Redegørelsen stilles til rådighed for de dataansvarlige offentlige afsendere.

Stk. 3. De dataansvarlige offentlige afsendere har ikke mulighed for at foretage inspektioner af Digitaliseringsstyrelsens fysiske faciliteter af ressourcemæssige og sikkerhedsmæssige grunde. Digitaliseringsstyrelsen udarbejder i stedet en redegørelse om databehandlingen, jf. stk. 2.

Stk. 4. Kontor for Revision og Tilsyn i Finansministeriets departement fører tilsyn med Digitaliseringsstyrelsen som databehandler på vegne af de dataansvarlige offentlige afsendere. Kontor for Revision og Tilsyn udarbejder en tilsynsrapport på baggrund af deres tilsyn, der stilles til rådighed for de dataansvarlige offentlige afsendere.

Stk. 5. Digitaliseringsstyrelsen skal give myndigheder, eller deres udpegede repræsentanter, der efter EU-retten eller lovgivningen i en medlemsstat har ret til adgang til den dataansvarlige og databehandlerens faciliteter, adgang til Digitaliseringsstyrelsens fysiske faciliteter mod forevisning af behørig legitimation.

Orientering af den anden part

§ 14. Digitaliseringsstyrelsen og de offentlige afsendere orienterer hinanden om væsentlige forhold, der har betydning for den behandling, der er omfattet af denne bekendtgørelse.

Ikrafttræden

§ 15. Finansministeren fastsætter tidspunktet for bekendtgørelsens ikrafttræden.