BEK nr 2020 af 29/10/2021 (Gældende)

Bekendtgørelse om ansvar, opgaver og tilsyn i forbindelse med behandlingen af personoplysninger indeholdt i meddelelser og opbevaringen heraf i juridiske enheders digitale postkasse

Ministerium: Digitaliseringsministeriet

Journalnummer: Finansmin., Digitaliseringsstyrelsen, j.nr. 2019 – 4329

Bekendtgørelse om ansvar, opgaver og tilsyn i forbindelse med behandlingen af personoplysninger indeholdt i meddelelser og opbevaringen heraf i juridiske enheders digitale postkasse

I medfør af § 2 a, stk. 5, i lov om Digital Post fra offentlige afsendere, jf. lovbekendtgørelse nr. 686 af 15. april 2021, fastsættes:

Anvendelsesområde

§ 1. Denne bekendtgørelse er udarbejdet af Digitaliseringsstyrelsen under henvisning til artikel 28 i Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (herefter databeskyttelsesforordningen) 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 juridiske enheder i forbindelse med opbevaringen og forsendelse af meddelelser indeholdende personoplysninger i den juridiske enheds digitale postkasse, jf. § 2 a, stk. 5, jf. stk. 4, i lov om Digital Post fra offentlige afsendere. Behandlingen sker for at den juridiske enhed har adgang til egen digital post fra offentlige afsendere, der opbevares i postløsningen, samt for at den juridiske enhed kan sende meddelelser via Digital Post.

Stk. 2. Juridiske enheders formål med databehandlingen fremgår af § 3, stk. 2, i lov om Digital Post fra offentlige afsendere, hvorefter juridiske enheder med cvr-nummer, jf. lov om Det Centrale Virksomhedsregister, skal tilsluttes Digital Post, med de retsvirkninger, der følger af lovens § 10.

Stk. 3. Juridiske enheder er dataansvarlige for behandlingen af de personoplysninger, der er indeholdt i og metadata tilknyttet meddelelser, de sender og opbevarer i Digital Post. Metadata omfatter i denne sammenhæng alene metadata, som de offentlige afsendere vælger at tilknytte deres meddelelser i forbindelse med afsendelsen og ikke metadata i form af administrationsdata, der muliggør selve opbevaringen og leveringen af meddelelser.

Stk. 4. Digitaliseringsstyrelsen er databehandler for de juridiske enheder, når disse sender og opbevarer meddelelser i Digital Post.

Stk. 5. Juridiske enheder 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, lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (herefter databeskyttelsesloven).

Stk. 6. Digitaliseringsstyrelsen og de dataansvarlige juridiske enheder 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, som f.eks. navn, adresse, kontaktoplysninger som e-mail og telefonnumre, stillingsbetegnelse m.v.
2) Særlige kategorier af personoplysninger (følsomme personoplysninger), i medfør af artikel 9, stk. 1 i databeskyttelsesforordningen, som f.eks. oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.
3) Personnumre.
4) Oplysninger om strafbare forhold, som f.eks. bøder, domme, sager for domstolene m.v.
5) CVR-numre der henviser til en enkeltmandsvirksomhed.

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 er modtaget fra offentlige afsendere og som de juridiske enheder sender via Digital Post.

Databehandleren handler efter instruks

§ 4. Digitaliseringsstyrelsen handler efter instruks fra den juridiske enhed. Digitaliseringsstyrelsen instrueres som databehandler i at modtage og sende meddelelser til offentlige afsendere og opbevare meddelelserne i den juridiske enheds digitale postkasse. Den dataansvarlige juridiske enhed kan give supplerende instruks, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk.

Stk. 2. Databehandleren underretter omgående den dataansvarlige juridiske enhed, hvis en instruks efter vedkommendes mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret. Instruksen vil fortsat have virkning indtil lovligheden af instruksen afklares af Digitaliseringsstyrelsen, bistået af den dataansvarlige juridiske enhed. Den dataansvarlige juridiske enhed forbliver ansvarlig for databehandlerens fortsatte behandling af personoplysninger.

Stk. 3. Denne bestemmelse udgør den databeskyttelsesretlige instruks i henhold til stk. 1. Nærmere oplysninger om selve behandlingen af personoplysninger fremgår af stk. 4 og henvisningerne i stk. 5. Omfanget af instruksen fremgår af henvisningerne i stk. 6.

Stk. 4. Digitaliseringsstyrelsens behandling af personoplysninger består af:
1) Transmission og levering af meddelelser med tilknyttede metadata sendt via Digital Post til de af de juridiske enheder anførte modtagere. Digitaliseringsstyrelsens behandling af personoplysninger på vegne af de juridiske enheder ophører således ved leveringen af meddelelserne til de af de juridiske enheder anførte modtageres digitale postkasser.
2) Opbevaring af de juridiske enheders meddelelser i Digital Post.

Stk. 5. Oplysninger om behandlingen af personoplysninger omfatter:
1) Formålet med behandlingen af personoplysninger, der fremgår af § 2, stk. 2.
2) Databehandlerens behandling af personoplysninger på vegne af de dataansvarlige juridiske enheder drejer sig om transmission og levering af meddelelser sendt via Digital Post og opbevaring af de juridiske enheders meddelelser i Digital Post, der fremgår af stk. 4.
3) Behandlingen omfatter følgende typer af personoplysninger om de registrerede, der fremgår af § 3, stk. 1.
4) Behandlingen omfatter følgende kategorier af registrerede, der fremgår af § 3, stk. 2.
5) Databehandlerens behandling af personoplysninger på vegne af de dataansvarlige juridiske enheder kan påbegyndes efter denne bekendtgørelses ikrafttræden. Behandlingen varer indtil bekendtgørelsen ophæves, jf. stk. 7.

Stk. 6. Den juridiske enhed instruerer Digitaliseringsstyrelsen som databehandler vedrørende behandlingen af personoplysninger. Instruksen omfatter:

1) Behandlingens genstand/instruks, der fremgår af stk. 1 og 3.
2) Behandlingssikkerhed, der fremgår af § 6.
3) Bistand til den dataansvarlige, der fremgår af § 10.
4) Opbevaring og sletning, der fremgår af § 12.
5) Lokalitet for behandlingen, der fremgår af stk. 8.
6) Instruks vedrørende overførsel af personoplysninger til tredjelande eller internationale organisationer, der fremgår af § 9.
7) Procedure for den dataansvarlige juridiske enheds revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandlere, der fremgår af § 13.
8) Procedure for den dataansvarlige juridiske enheds revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til underdatabehandlere, der fremgår af § 8, stk. 6.

Stk. 7. Digitaliseringsstyrelsens behandling af personoplysninger i Digital Post på vegne af de juridiske enheder er ikke tidsbegrænset, men varer indtil bekendtgørelsen ophæves, eller indtil de juridiske enheder sletter meddelelser i deres egen digitale postkasse.

Stk. 8. Digital Post-løsningen er omfattet af lokationskravet i databeskyttelseslovens § 3, stk. 9, og bestemmelser udstedt i medfør heraf, hvorefter personoplysninger, der behandles i nærmere bestemte it-systemer, og som føres for den offentlige forvaltning, helt eller delvis alene må opbevares her i landet. Behandlingen og opbevaringen af personoplysninger skal ske i Danmark på baggrund af 1. pkt.

Fortrolighed

§ 5. Digitaliseringsstyrelsen skal som databehandler sikre, at de personer, der er autoriseret til at behandle personoplysninger på vegne af de juridiske enheder, 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 på baggrund af en risikovurdering. Digitaliseringsstyrelsen sikrer herved, at der under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici. Digitaliseringsstyrelsen stiller på sin hjemmeside en sammenfatning af den foretagne risikovurdering til rådighed for de dataansvarlige juridiske enheder, så risikovurderingen kan indgå i de dataansvarliges egne risikovurderinger.

Stk. 2. Digitaliseringsstyrelsen gennemfører passende foranstaltninger for at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og tjenester ved at imødegå de i risikovurderingen identificerede risici. Der kan alt efter, hvad der er relevant, være tale om følgende foranstaltninger:

1) Kryptering af personoplysninger.
2) Logning af brug og adgang til personoplysninger.
3) Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af fysisk eller teknisk hændelse.
4) En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

Stk. 3. Digitaliseringsstyrelsen fastsætter på baggrund af risikovurderingen, jf. § 6. stk. 1, og forslag til passende foranstaltninger, jf. § 6, stk. 2, nærmere interne bestemmelser om tekniske og organisatoriske sikkerhedsforanstaltninger, i eget informationssikkerhedsledelsessystem, for databehandlingen.

1) De interne bestemmelser gennemgås mindst én gang hvert år med henblik på at sikre, at de er fyldestgørende, og afspejler de faktiske forhold hos Digitaliseringsstyrelsen i rollen som databehandler.
2) Digitaliseringsstyrelsen giver den fornødne instruktion til egne medarbejdere, som behandler personoplysninger. Medarbejderne skal herunder gøres bekendt med de regler, der er fastsat i medfør af dette afsnit.

Stk. 4. Den enkelte juridiske enhed er ansvarlig for at gennemføre egne relevante organisatoriske og tekniske sikkerhedsforanstaltninger, som knytter sig til den juridiske enheds rolle som dataansvarlig i forbindelse med anvendelsen af Digital Post.

Stk. 5. 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. De nærmere retningslinjer for denne autoriseringsordning er fastsat i dette afsnit.

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

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

Stk. 4. Kontrol af, hvorvidt de autoriserede personer fortsat skal have adgang til personoplysningerne, skal ske når det findes nødvendigt og mindst én gang hvert år.

Anvendelse af underdatabehandlere

§ 8. Digitaliseringsstyrelsen har generel godkendelse til at anvende underdatabehandlere til Digital Post. Databehandleren vil underrette den dataansvarlige juridiske enhed på Digitaliseringsstyrelsens hjemmeside om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst en måneds varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e).

Stk. 2. Ved anvendelse af underdatabehandlere er Digitaliseringsstyrelsen ansvarlig for at efterleve kravene i databeskyttelsesforordningens artikel 28. 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 juridiske enheder 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 revisorerklæring i overensstemmelse med aktuelle standarder for GDPR-revisorerklæringer fra en uafhængig revisor angående underdatabehandleren og dennes eventuelle underdatabehandleres behandling af informationssikkerhed og personoplysninger i medfør af den til enhver tid gældende underdatabehandleraftale. Digitaliseringsstyrelsen modtager revisorerklæringen fra underdatabehandleren, hvorefter den stilles til rådighed for de dataansvarlige juridiske enheder.
2) Digitaliseringsstyrelsen, eller en uafhængig revisor bemyndiget af Digitaliseringsstyrelsen, har ret til at foretage inspektioner af underdatabehandlerens fysiske faciliteter, hvor der behandles personoplysninger samt modtage de nødvendige informationer til udførelsen af undersøgelsen af, hvorvidt underdatabehandleren har truffet de sikkerhedsforanstaltninger, der følger af underdatabehandleraftalen samt gældende databeskyttelsesret.
3) Digitaliseringsstyrelsen har løbende mulighed for at indhente informationer baseret på resultaterne af enten revisorerklæringen, inspektionen af de fysiske faciliteter eller de modtagende informationer. Når der er behov for det, er Digitaliseringsstyrelsen berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og denne bekendtgørelse.
4) Underdatabehandleren skal give myndigheder, eller deres udpegede repræsentanter, der efter EU-retten eller lovgivningen i en medlemsstat har ret til adgang til Digitaliseringsstyrelsens og underdatabehandlerens faciliteter, adgang til underdatabehandlerens fysiske faciliteter mod forevisning af behørig legitimation.

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

Overførsel til tredjelande eller internationale organisationer

§ 9. Digitalisereringsstyrelsen vil som databehandler for Digital Post ikke overføre personoplysninger til tredjelande eller internationale organisationer, jf. § 4, stk. 7.

Stk. 2. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af Digitaliseringsstyrelsen på baggrund af dokumenteret instruks herom fra den dataansvarlige juridiske enhed og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V. Uden dokumenteret instruks fra den dataansvarlige juridiske enhed kan Digitaliseringsstyrelsen således ikke inden for rammerne af denne bekendtgørelse:

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

Stk. 3. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som Digitaliseringsstyrelsen ikke er blevet instrueret i at foretage af den dataansvarlige juridiske enhed,

kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Digitaliseringsstyrelsen er underlagt, skal Digitaliseringsstyrelsen underrette den dataansvarlige juridiske enhed om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

Stk. 4. Ved overførsler omfattet af stk. 2, er den juridiske enhed 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 juridiske enhed ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den juridiske enheds forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder, som er fastlagt i databeskyttelsesforordningens kapitel III.

Stk. 2. Digitaliseringsstyrelsen skal i medfør af stk. 1, så vidt muligt skal bistå den juridiske enhed i forbindelse med, at den juridiske enhed i dens rolle som dataansvarlig skal sikre overholdelsen af nedenstående regler i databeskyttelsesforordningen:

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

Stk. 3. Digitaliseringsstyrelsen bistår den juridiske enhed med at sikre overholdelse af den dataansvarliges 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 juridiske enhed i forbindelse med, at denne skal sikre overholdelsen af:

1) Forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen, jf. § 6.
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 juridiske enhed efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

Stk. 2. Digitaliseringsstyrelsens underretning til den dataansvarlige juridiske enhed skal ske uden unødig forsinkelse og senest 48 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige juridiske enhed kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til Datatilsynet, jf. databeskyttelsesforordningens artikel 33. Den juridiske enhed 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 juridiske enheder 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. Digitaliseringsstyrelsen underretter uden unødig forsinkelse den dataansvarlige juridiske enhed efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden, og inden en samlet anmeldelse sendes til Datatilsynet.

Stk. 4. I overensstemmelse med stk. 1 skal Digitaliseringsstyrelsen bistå den juridiske enhed 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 juridiske enheds anmeldelse af bruddet til Datatilsynet:

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

Sletning af personoplysninger

§ 12. Digitaliseringsstyrelsens databehandling i medfør af denne bekendtgørelse ophører:

1) Ved tranmission og levering af meddelelser til de af de juridiske enheder anførte modtageres digitale postkasse.
2) Når den juridiske enhed ikke længere opbevarer egne meddelelser i Digital Post.

Stk. 2. Digitaliseringsstyrelsen sletter ikke de i § 3 nævnte personoplysninger, da meddelelserne efter levering er overgået til modtagernes råde- og ejendomsret.

Stk. 3. Digitaliseringsstyrelsen opbevarer de meddelelser, som modtagerne, en fysisk person eller en juridisk enhed, har i sin digitale postkasse, indtil modtageren selv vælger at slette meddelelsen fra sin digitale postkasse.

Tilsyn og revision

§ 13. Digitaliseringsstyrelsen stiller alle oplysninger, der er relevante og nødvendige for at påvise overholdelse af kravene i bekendtgørelsen, til rådighed for de dataansvarlige juridiske enheder, 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 juridiske enheder.

Stk. 3. De dataansvarlige juridiske enheder 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. De dataansvarlige juridiske

enheder har dog mulighed for at anmode om supplerende oplysninger om Digitaliseringsstyrelsens databehandling, ligesom alle relevante oplysninger vil blive stillet til rådighed for de dataansvarlige juridiske enheder på Digitaliseringsstyrelsens hjemmeside, jf. stk. 1 og 2.

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

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 juridiske enheder orienterer hinanden om væsentlige forhold, der har betydning for den behandling, der er omfattet af denne bekendtgørelse.

Ikrafttræden

§ 15. Bekendtgørelsen træder i kraft den 25. november 2021.

Finansministeriet, den 29. oktober 2021

Nicolai Wammen

/ Tanja Franck