Til Digitaliseringsstyrelsen

Forsikring & Pension

Forsikring & Pensions høringssvar vedr. Digitaliseringsstyrelsens to bekendtgørelser om behandling af persondata i Digital Post fra offentlige afsendere

04.02.2021

Forsikring & Pension
Philip Heymans Allé 1
2900 Hellerup
Tlf.: 41 91 91 91
fp@forsikringogpension.dk
www.forsikringogpension.dk

Karen Gjølbo
Chefkonsulent
Dir. 41919045
kgj@forsikringogpension.dk

Sagsnr. GES-2021-00018
DokID 418990

Vi vil gerne takke for muligheden for at kommentere på bekendtgørelserne. Forsikring & Pensions høringssvar berører umiddelbart alene *bekendtgørelsen om ansvar, opgaver og tilsyn for behandlingen af personoplysninger indeholdt i meddelelser og opbevaringen heraf i juridiske enheders digitale postkasse.*

Overordnet støtter Forsikring & Pension udviklingen af Digital Post-løsningen og det fortsatte fokus på at sikre brugervenligheden og sikkerheden i løsningen, der samtidig gør kommunikationen med det offentlige mere smidigt både for borgere og virksomheder.

Vi noterer os, at Digitaliseringsstyrelsen også har fokus på, at løsningen kan tilpasses til fremtidige behov. Forsikring & Pension vil i den forbindelse 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. Der kan være grund til at se på, om denne kommunikation ikke også kunne smidiggøres.

I forhold til Digital Post-løsningen for offentlige afsendere, så finder vi det umiddelbart positivt, at rollefordelingen mellem dataansvarlig og databehandler i den nye løsning på forhånd er gjort klar, og at der med bekendtgørelsen sikres en regulering af forholdet. Vi ser dog også udfordringer i denne model. Det skyldes, at reguleringen sætter rammerne for databehandlingen efter databeskyttelsesforordningen, men er upræcis og indebærer en række begrænsninger i de dataansvarliges rettigheder og mulighed for at føre tilsyn med databehandleren og dennes underdatabehandlere. Dette giver anledning til følgende specifikke bemærkninger, som Digitaliseringsstyrelsen bør nærmere tage stilling til:

(Instruks)

- Den dataansvarlige har efter databeskyttelsesforordningen pligt til at give instruks til databehandlerens, og databehandlere kun må handle efter instruks fra den dataansvarlige. Digitaliseringsstyrelsen bør tage nærmere stilling til, hvordan kravet om instruks opfyldes i denne bekendtgørelse.

(Behandlingssikkerhed og fortrolighed)

- Der er behov for en præcisering af hvilke data der er adgang til for Digitaliseringsstyrelsen, herunder om det alene er metadata genereret ved forsendelserne eller er der også adgang til data i selve de dokumenter, der sendes via løsningen. Sidstnævnte burde ikke være nødvendigt for håndtering af løsningen og derfor heller ikke muligt.

- Afhængig af omfanget og karakteren af personoplysninger, der er adgang til i løsningen, bør det klart 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.

- Af § 10, stk. 3, nr. 4) i udkastet fremgår det, at Digitaliseringsstyrelsen skal bistå med at foretage 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 det er de enkelte dataansvarlige hver især skal foretage en sådan. Dette bør herefter afspejles i bekendtgørelsen.

(Anvendelse af underdatabehandlere)
Bekendtgørelsen indeholder ikke ret for den dataansvarlige til at godkende og gøre indsigelse mod Digitaliseringsstyrelsens underdatabehandlere, da 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 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 præciseres, hvor disse oplysningerne kan findes på styrelsens hjemmeside, og der bør som minimum ske notifikation, hvis der sker ændringer i underdatabehandlerne.

- Digitaliseringsstyrelsen bør samtidig oplyse om brugen af underdatabehandlernes eventuelle underdatabehandlere.

- Det bør ligeledes fremgå af Digitaliseringsstyrelsens hjemmeside, hvor data opbevares (lokation).

- Digitaliseringsstyrelsens tilsyn med deres underdatabehandlere sker bl.a. gennem fremsendelse af en årlig revisorerklæring fra en uafhængig revisor. Det bør klart fremgå, hvilken standard revisorerklæringen skal baseres på (Fx ISAE 3000 og/eller ISO 277001) og at den skal stilles til rådighed for de dataansvarlige.

- Det bør fremgå af bekendtgørelsen, at Digitaliseringsstyrelsen skal imødekomme de dataansvarliges begrundede rimelige krav om yderligere sikkerhedsforanstaltninger i forhold til underdatabehandlerne fx som følge af konstateret databrud og sikkerhedsbrist hos underdatabehandleren; den fremsendte revisorerklæring, nye regler eller skærpet praksis mv.

(Tilsyn og kontrol af databehandleren)

- 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 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.

- Efter udkastets § 10 Digitaliseringsstyrelsen er berettiget til at videregive metadata fra Digital Post til brug for udførelse af f.eks. statistiske eller videnskabelige undersøgelser, når den rekvirerende aktør efter lovgivningen har hjemmel hertil til sådanne formål. Efter Forsikring og Pensions vurdering bør en sådan videregivelse af data kun kunne ske mod forudgående høring Det er desuden ikke klart, hvilke data, der omfattes af termen metadata, som dermed kan videregives. Det bør præciseres.

- 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 præciseres, at dette "*skal* ske" senest 48 timer efter, at Digitaliseringsstyrelsen er blevet bekendt med bruddet.

(Overførsel af data til tredjelande)

- Som udgangspunkt kan der kun 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. Det vil i den forbindelse være afgørende at den dataansvarlig er i 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.

Forsikring og Pension står selvfølgelig til rådighed for eventuel uddybning af de fremførte bemærkninger fra branchen.

Med venlig hilsen

Karen Gjølbo