EU DATABESKYTTELSESFORORDNING

MaJ 2018

Vejledning om tilsyn med databehandlere og underdatabehandlere

IMG

DATATILSYNET

Vejledende tekst om tilsyn med databehandlere og underdatabehandlere

Maj 2018

Baggrunden for den vejledende tekst

Det er Datatilsynets erfaring, at en del dataansvarlige har haft udfordringer i forhold til 1) at få indgået skriftlige databehandleraftaler med sine databehandlere samt 2) at få påset behandlingssikkerheden hos sine databehandlere.

For at afhjælpe udfordringerne i forhold til at få indgået de fornødne databehandleraftaler har Datatilsynet i februar 2018 offentliggjort en standard-databehandleraftale. Aftalen er tænkt som en hjælp til dataansvarlige og databehandlere, der skal efterleve databeskyttelsesforordningens krav om at indgå en skriftlig databehandleraftale med et vist minimumsindhold. Standarddata-behandleraftalen og den medfølgende tekst kan ses her:

https://www.datatilsynet.dk/media/6815/standard-databehandleraftale.docx og https://www.datatilsynet.dk/media/6812/databehandleraftale_-_foelgetekst.pdf. Standarddatabehandleraftalen findes i øvrigt også i en engelsk version, som kan ses her: https://www.datatilsynet.dk/media/6814/dpa-template.docx.

For så vidt angår udfordringerne i forhold til at få påset behandlingssikkerheden hos sine databehandlere redegøres der i det følgende for, hvorfor det er nødvendigt at påse behandlingssikkerheden hos sine databehandlere, ligesom der redegøres for, hvem der kan påse behandlingssikkerheden, hvordan behandlingssikkerheden kan påses, og hvor ofte behandlingssikkerheden bør påses.

Hvorfor er det nødvendigt at påse behandlingssikkerheden hos sine databehandlere?

Datatilsynet har erfaret, at der i forbindelse med myndigheders og virksomheders arbejde med at leve op til reglerne i databeskyttelsesforordningen er blevet stillet spørgsmålstegn ved, om det stadig er et krav, at den dataansvarlige påser behandlingssikkerheden hos sine databehandlere. Baggrunden herfor er, at kravet ikke fremgår af en konkret bestemmelse i databeskyttelsesforordningen.

Selvom det ikke fremgår eksplicit af en bestemmelse i databeskyttelsesforordningen, at man skal påse behandlingssikkerheden hos sine databehandlere, er det Datatilsynets opfattelse, at man også nu her, hvor forordningen finder anvendelse, skal påse behandlingssikkerheden hos sine databehandlere.

Baggrunden herfor er, at den dataansvarlige skal leve op til kravet om ansvarlighed og skal kunne påvise, at en behandling af personoplysninger er i overensstemmelse med reglerne i databeskyttelsesforordningen. Den dataansvarlige vil – efter Datatilsynets opfattelse – ikke kunne leve op til ovenstående krav ved blot at indgå en databehandleraftale med databehandleren. Den dataansvarlig må således også føre et (større eller mindre) tilsyn med, at den indgåede databehandleraftaler overholdes, herunder at databehandleren har gennemført de aftalte tekniske og organisatoriske sikkerhedsforanstaltninger.

Hvem kan påse behandlingssikkerheden hos en databehandler?

Grundlæggende kan man som dataansvarlig vælge 1) selv at påse behandlingssikkerheden hos sine databehandlere eller 2) vælge at få en ekstern uafhængig tredjepart (f.eks. et revisionsselskab) til at påse behandlingssikkerheden hos sine databehandlere.

Om man vælger den ene eller den anden model vil bl.a. afhænge af, hvor kompleks en databehandlerkonstruktion er, og om den dataansvarlige selv har medarbejdere, der har den fornødne IT-sikkerhedsmæssige viden til at påse, om en databehandler har gennemført de aftalte tekniske og organisatoriske sikkerhedsforanstaltninger.

Er en databehandlerkonstruktion mindre kompleks, kan en dataansvarlig, der ikke selv har den fornødne IT-sikkerhedsmæssige viden – som en slags kombination af de to skitserede modeller – også vælge at indhente hjælp fra en ekstern rådigiver (revisor, advokat mv.) til at få formuleret nogle spørgsmål, som den dataansvarlige selv kan benytte til at påse behandlingssikkerheden hos sine databehandlere.

Hvis man derimod vælger at lade en uafhængig ekstern tredjepart påse behandlingssikkerheden (eventuelt efter databehandlerens ønske), er det meget vigtigt, at man som dataansvarlig sikrer sig, at den eksterne tredjepart rent faktisk påser, at databehandleren har gennemført de aftalte tekniske og organisatoriske sikkerhedsforanstaltninger. Datatilsynet har i forbindelse med flere tilsyn set eksempler på, at en valgt ekstern tredjepart har påset ting, der ikke er relevante i forhold til de aftalte foranstaltninger. I sådanne situationer vil tilsynet med databehandleren derfor ikke være tilstrækkeligt.

Hvordan kan man påse behandlingssikkerheden hos en databehandler?

Efter databeskyttelsesforordningens artikel 32 skal den dataansvarlige og databehandleren gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen.

Af databeskyttelsesforordningens artikel 28, stk. 3, litra c, følger det endvidere, at det skal fremgå af en databehandleraftale, at databehandleren gennemfører de foranstaltninger, der kræves i henhold til artikel 32.

Hvilket sikkerhedsniveau, det er nødvendigt at gennemføre hos databehandleren, afhænger af en vurdering, som den dataansvarlige og databehandleren skal foretage, hvor der navnlig skal tages hensyn til de risici, som behandling af personoplysninger vil have for de registrerede ("risikovurderingen").

Den dataansvarlige og databehandleren skal derfor – før behandlingens begyndelse – tage stilling til, hvilke sikkerhedsforanstaltninger der skal gennemføres hos databehandleren. Afklaringen heraf skal herefter afspejles i parternes databehandleraftale.

Når omdrejningspunktet for den dataansvarliges tilsyn med sine databehandlere er databehandlerens overholdelse af databehandleraftalen, er det naturligt, at den dataansvarliges tilsyn med sikkerheds-niveauet hos databehandleren, også tager udgangspunkt i de sikkerhedsforanstaltninger, der er aftalt.

I praksis kan den dataansvarlige således med fordel tage udgangspunkt i den konkrete aftale og planlægge sine tilsyn på baggrund af det sikkerhedsniveau, der er beskrevet i aftalen.

For så vidt angår selve formen af et tilsyn med en databehandler, da kan et sådan tilsyn både ske ved fysiske besøg hos databehandleren og ved skriftlig informationsindsamling mv.

Ved valget af tilsynsformen, vil en dataansvarlig skulle skele til den risikovurdering, som den dataansvarlige har foretaget. Tilsynsformen afhænger således af den identificerede risiko. Hvis risikoen for de registreredes rettigheder er høj, kan det være nødvendigt at føre fysiske tilsyn med sine databehandlere, ligesom det – alt efter omstændighederne – kan være tilstrækkeligt, hvis risikoen er lav, at føre skriftligt tilsyn.

Brugen af et fysisk tilsyn, hvor den dataansvarlige kommer til stede på den lokation hvor databehandleren behandler de omhandlede personoplysninger, skal afspejle de risikoscenarier, som den dataansvarlige har konstateret i forbindelse med sin risikovurdering. Det kan f.eks. være, at den dataansvarlige, i sin risikovurdering, har anført fysiske tilsyn som en foranstaltning, der kan begrænse risikoen, ligesom det kan være anført, at en effektiv stikprøvekontrol alene kan foretages ved fysiske tilsyn. Det kan også være at den dataansvarlige, mere generelt i forbindelse med sit risikobaserede sikkerhedsarbejdet, har vurderet, at fysiske tilsyn er at foretrække.

Som eksempler på momenter i en risikovurdering, som kan tale for fysiske tilsyn, kan bl.a. peges på delegation og brug af administrative rettigheder, adgangen til persondata, konkrete opsætninger og indstillinger af den fysiske infrastruktur, efterlevelse af konkrete tekniske foranstaltninger, pålagte sletteregler, overholdelse af konkrete organisatoriske forholdsregler, herunder den fysiske sikkerhed eller databaggrunden for det skriftlige materiale der på mere daglig basis danner grundlaget for opfølgningen på det niveau af behandlingssikkerhed, der er aftalt mellem parterne.

Et skriftligt tilsyn kan f.eks. ske i form af løbende afrapporteringer fra databehandleren i forhold til de parametre, som med risikovurderingen er vurderet som værende påkrævede. Disse afrapporteringer kan f.eks. være baseret på et subset af SANS Critical Security Controls, ISO 27007 eller andre typer af kontroller, der kan rapporteres omkring på skrift. Der kan også foretages stikprøver og temakontroller over de kontrolregimer, der måtte afspejle den dataansvarliges risikovurdering.

<u>Hvor ofte skal man påse behandlingssikkerheden hos sine databehandlere?</u>

Et andet spørgsmål, som Datatilsynet ofte bliver mødt med, er, hvor ofte det er nødvendigt for den dataansvarlige at påse behandlingssikkerheden hos sine databehandlere.

Dette vil ligeledes afhænge af den risikovurdering, som den dataansvarlige har foretaget.

Hyppigheden vil derfor afhænge af den identificerede risiko. Hvis risikoen for de registreredes rettigheder er høj, kan det være nødvendigt at påse behandlingssikkerheden hos sine databehandlere årligt eller endda halvårligt, ligesom det – alt efter omstændighederne – kan være tilstrækkeligt, hvis risikoen er lav, at påse behandlingssikkerheden med en lavere frekvens.

I et miljø med en stor dynamisk udvikling i leveranceplatformen og applikationsporteføljen og i et miljø hvor den benyttede infrastruktur er eksponeret for hurtigt skiftende risikoscenarier, vil der

være behov for hyppigere og mere målrettet kontrol, end i et miljø, der er mere statisk, og hvor der er en på forhånd kendt og ikke fluktuerende risiko.

Hvordan påses behandlingssikkerheden hos eventuelle underdatabehandlere?

Hvis en dataansvarlig godkender, at dennes databehandler må anvende en anden databehandler (underdatabehandler), skal den oprindelige databehandler sørge for at pålægge underdatabehandleren de samme databeskyttelseskrav som dem, der fremgår af den oprindelige databehandleraftale mellem den dataansvarlige og den oprindelige databehandler. Det er således i udgangspunktet databehandleren, der sikrer indgåelsen af en underdatabehandleraftale.

Kravet om, at der skal føres tilsyn med behandlingen af personoplysninger hos en underdatabehandler følger – ligesom det er tilfældet med den oprindelige databehandler – ikke af en konkret bestemmelse i databeskyttelsesforordningen. Efter Datatilsynets opfattelse vil den dataansvarlige imidlertid heller ikke være i stand til at kunne påvise efterlevelse af databeskyttelsesforordningen, hvis den dataansvarlige ikke er vidende om, hvorvidt underdatabehandleren handler inden for rammerne af underdatabehandleraftalen (og hermed den oprindelige databehandleraftale).

De praktiske muligheder for at føre tilsyn med en underdatabehandler og hvad der i den konkrete situation vil udgøre et tilstrækkeligt tilsyn, må afgøres efter de samme principper, som tilsynet med databehandleren, jf. det ovenfor nævnte.

Dog lægges der med forordningen op til, at det som udgangspunkt overlades til databehandleren at føre tilsyn med en underdatabehandler. Dette harmonerer godt med, at det er den oprindelige databehandler, som har et aftale-forhold med underdatabehandleren. Det bør derfor også være den oprindelige databehandler, der er ansvarlig for – overfor den dataansvarlige – at sørge for, at underdatabehandleren lever op til sine databeskyttelsesforpligtelser.

Den dataansvarlige skal imidlertid sikre sig, at databehandleren fører det aftalte tilsyn med underdatabehandleren. Dette kan f.eks. ske ved, at databehandleren sender dokumentation for afholdte tilsyn til den dataansvarlige.