FOLKETINGET

Erhvervsudvalget, Retsudvalget og Europaudvalget

EU-konsulenterne

Til: Udvalgets medlemmer
Dato: **22. november 2017**

Kontaktperson:

Julia Ballaschk (3655)

Supplerende oplysninger til EU-noten om nye databeskyttelsesregler for virksomheder

Sammenfatning
EU's databeskyttelsesforordning, der træder i kraft den 25. maj 2018, ændrer en række regler, der gælder for virksomhedernes behandling af personoplysninger. EU-noten om nye databeskyttelsesregler for virksomheder skitserer nogle af de vigtigste ændringer og nyskabelser i forordningen. Da der er blevet stillet nogle spørgsmål om bl.a. dokumentationskravet og bødeniveauet, uddyber dette supplement til noten nogle af de vigtigste ændringer i forordningen. Navnlig forordningens dokumentationskrav, kravet om konsekvensanalyse og forordningens bødebestemmelserne.

Dokumentationskrav for virksomheder

Den hidtil gældende databeskyttelseslovgivning krævede, at indsamling og behandling af personoplysninger i visse situationer skulle anmeldes til Datatilsynet (jf. art. 18, stk. 1 i direktiv 95/46/EF og persondatalovens §§ 43, stk. 1 og 48). Denne anmeldelse skulle indeholde en optegnelse over de behandlingsaktiviteter, der anmeldtes. Derudover forpligter persondatalovens § 54, stk. 2 den dataansvarlige allerede på nuværende tidspunkt til at være i stand til at på anmodning udlevere en oversigt til enhver over alle behandlingsaktiviteter.

Persondataforordningen erstatter anmeldelseskravet med et *internt* dokumentationskrav (jf. forordningens art. 30). Herunder forstås kravet om at føre behandlingsfortegnelser. Kravet gælder som noget nyt også for databehandlere. Behandlingsfortegnelserne skal være elektronisk og skriftlig og indeholde en række oplysninger.[1]

Efter Justitsministeriets vurdering er der ikke holdepunkter for at antage, at forordningens fortegnelseskrav indebærer krav i meget videre omfang, end hvad der kendes fra omfanget af anmeldelserne efter databeskyttelsesdirektivet og persondataloven.[2] Ifølge Justitsministeriet er forordningens art. 30 ikke tiltænkt som "belastning" for den dataansvarlige eller databehandleren og medfører ikke i sig selv et krav om udarbejdelse af større analyser eller datastrømme.

Undtagelser fra dokumentationskrav

Virksomheder eller organisationer, der beskæftiger under 250 ansatte er ikke underlagt pligten til at føre fortegnelser, jf. forordningens art. 30, stk. 5, medmindre behandlingen medfører høj risiko eller omfatter følsomme data (art. 9 og 10 i forordningen). Det er uklart, hvor mange små og mellemstore virksomheder vil være omfattet af undtagelsesbestemmelsen. Justitsministeriet vurderer, at den i praksis vil få et snævert anvendelsesområde.[3]

Andre former for dokumentation

Den dataansvarlige skal til enhver tid kunne påvise sin overholdelse af de almindelige principper for persondatabehandling og implementere tekniske og organisatoriske foranstaltninger, som sætter den dataansvarlige i stand til at påvise, at påvise, at dennes persondatabehandling er i overensstemmelse

---

[1] Dokumentationen skal mindst omfatte:
- Navn og kontaktoplysninger på den dataansvarlige eller den fælles dataansvarlige og dennes eventuelle repræsentant samt evt. DPO
- Formålene med behandlingen
- Beskrivelse af kategorier af datasubjekter og kategorier af personoplysninger vedrørende datasubjekter
- Kategorier af modtagere af personoplysningerne
- Evt. overførsel af personoplysninger til et tredjeland, herunder identifikation af dette tredjeland, og dokumentation af fornødne garantier ved overførsel til ikke-sikre tredjelande
- En generel angivelse af tidsfristerne for sletning af de forskellige kategorier af personoplysninger
- Hvis muligt, en beskrivelse de tekniske og organisatoriske sikkerhedsforanstaltninger

[2] Betænkning nr. 1565 s. 460.

[3] Betænkning nr. 1565 s. 465. Desuden: Peter Blume, Den nye persondataret, s. 117.

med forordningens krav, jf. forordningens art. 24. Forordningen præciserer ikke nærmere, hvilke foranstaltninger, der vil være passende. Justitsministeriet henviser i sin betænkning til Artikel 29-gruppens udtalelse om princippet for ansvarlighed og nævner bl.a. kortlægning af procedurer, uddannelse af personale eller etablering af interne procedurer som typer af konkrete foranstaltninger, der kan sikre efterlevelse af regler.[4] Desuden kan der bruges certificeringsforanstaltninger, jf. forordningens art. 42.[5] Nogle praktikere mener, at princippet om ansvarlighed i praksis vil kræve udarbejdelse af dokumentation.[6]

Risikovurdering og konsekvensanalyser

Som beskrevet ovenfor skal efter gældende ret al persondatabehandling anmeldes til Datatilsynet, jf. Persondatalovens kapitel 12 og 13. Forordningen erstatter dette bredt dækkende krav med en risikobaseret tilgang, og tager udgangspunkt i, at der kun skal foretages særlige foranstaltninger, når der foreligger en høj risiko for, at persondatabehandlingen kan krænke den registrerede.[7] Forordningen kræver derfor, at den dataansvarlige foretager en risikoanalyse hver gang persondata behandles for at fastsætte et passende niveau af teknisk og organisatorisk sikkerhed.

Er der tale om behandling af personoplysninger med høj risiko for de registreredes rettigheder, skal den dataansvarlige gennemføre en konsekvensanalyse (jf. art. 35).

En konsekvensanalyse skal altid foretages, hvis

- Der er tale om profiling (systematisk og omfattende vurdering af personlige forhold ved brug af automatiseret behandling)
- Behandling af helbredsoplysninger mhp. at træffe foranstaltninger eller beslutninger vedr. bestemte grupper
- Overvågning af offentligt tilgængelige områder, navnlig ved omfattende brug af videoovervågning

En konsekvensanalyse skal bl.a. indeholde en systematisk beskrivelse af den påtænkte persondatabehandling, de formål, der ligger bag og de interesser, den dataansvarlige lægger til grund. Endelig skal den også beskrive de sikkerhedsforanstaltninger, der skal træffes.

---

[4] Betænkning nr. 1565 s. 407-408.

[5] Bertermann: Verantwortung des für die Verarbeitung Verantwortlichen, i: Ehmann/Selmayr: Datenschutzgrundverordnung, s. 542.

[6] Dall, Langemark, Langebæk: Persondataforordningen – en håndbog for praktikere, s. 87.

[7] Blume, s. 124-125.

Forordningens art. 36, stk. 1 kræver også at den dataansvarlige skal høre repræsentanter for den registrerede, såfremt det er relevant (f.eks. forbrugerbeskyttelsesgrupper). Hvis konsekvensanalysen viser, at der er en høj risiko ved den påtænkte behandling, skal den dataansvarlige høre Datatilsynet.

Konsekvensanalyser er ikke reguleret i gældende ret, men er blevet anbefalet af Datatilsynet i specifikke situationer og gennem vejledninger fra Digitaliseringsstyrelsen. Ligeledes finder der regler om forudgående høring af tilsynsmyndigheden.[8]

Bøder

Det hidtil gældende databeskyttelsesdirektiv har kun meget overordnet reguleret brugen af sanktioner, hvilket har resulteret i et meget forskelligt bødeniveau i EU-medlemslandene.

Forordningen indfører to bødeniveauer. Det maksimale bødeniveau er 10 mio. euro eller op til 2 pct. af sidste års verdensomsætning for bl.a. følgende overtrædelser, jf. forordningens art. 83, stk. 4a:

- overtrædelse af reglerne om børns samtykke ved brug af informationssamfundstjenester
- overtrædelse af sikkerhedskrav
- overtrædelse om krav om konsekvensanalyse
- overtrædelse om krav om databeskyttelsesrådgiver

Artikel 83, stk. 5 opregner de alvorligste overtrædelser, hvor bødeniveauet kan gå op til 20 million euro eller 4 pct. af virksomhedens årlige verdensomsætning. Denne sanktion gælder for overtrædelsen af de grundlæggende principper og behandlingsprincipper, såsom:

- rettighedsreglerne
- reglerne om dataoverførsler
- tilsynets påbud eller pligten til at give adgang ved inspektioner.

De i forordningen nævnte bøder er maksima, og lavere bøder kan anvendes. Justitsministeriet vurderer dog, at bestemmelsen vil betyde en væsentlig forøgelse af bødestørrelsen i forhold til, hvad overtrædelser af persondataloven i dag takseres til.[9] Peter Blume konstaterer dog, at Danmark i dag er et af de billigste lande ift. sanktionsniveauet.[10]

---

[8] Betænkning nr. 1565, s. 534, 542.

[9] Betænkning nr. 1565, s. 927.

[10] Blume, s. 162.