Moalem Weitemeyer Bendtsen
Advokatpartnerselskab

8. marts 2012

J.nr.: 243976

FORSLAG TIL REFORM AF EU'S PERSONDATABESKYTTELSESREGLER

Indledning

Kommissionen foreslog den 25. januar 2012 en omfattende reform af persondatabeskyttelsesreglerne. Sigtet med EU's persondatabeskyttelsesregler er både at beskytte fysiske personers grundlæggende rettigheder og friheder og at sikre en fri udveksling af data inden for EU.

Kommissionens forslag til forordning ajourfører og moderniserer de principper, der er fastslået i det eksisterende databeskyttelsesdirektiv fra 1995 (95/46/EF) og søger at tage højde for den teknologiske udvikling, hvor omfanget af datadeling og -indsamling er steget drastisk.

De væsentligste ændringer helt kort

De væsentligste ændringer er:

- Virksomheder med mere end 250 ansatte skal ansætte en databeskyttelsesansvarlig (DPO)
- Pligt til at underrette myndigheder og berørte ved brud på persondatasikkerheden
- Bødeniveauet hæves til op til 2 % af en virksomheds globale omsætning ved overtrædelse af persondatareglerne

Der er endnu alene tale om et forslag, men der er tale om ændringer, som med stor sandsynligvis vil blive gennemført om nogle år, og som man som virksomhed allerede

Amaliegade 3-5
DK-1256 København K

Tel: +45 7070 1505
Fax: +45 7070 1506
Mail: info@mwblaw.dk
Web: www.mwblaw.dk

CVR: 3162 7885

bør have i baghovedet i forhold til virksomhedens forskellige IT-systemer og processer til behandling af personoplysninger.

Forslaget til forordningen uddybet

De vigtigste ændringer i forhold til de nugældende regler i forslaget til forordningen gennemgås kort her:

Præcisering af det geografiske anvendelsesområde

Registreringsansvarlige etableret i lande uden for EU er allerede omfattet af databeskyttelsesdirektivet. Kommissionens forslag præciserer, hvornår en registreringsansvarlig, som er etableret uden for EU, er omfattet. Det vil de være, såfremt behandlingsaktiviteterne vedrører a) udbud af varer eller tjenester til EU-borgere eller b) overvågning af EU-borgeres adfærd.

Formålet har navnlig været at få Facebook og lignende udenlandske tjenester omfattet af EU-regulering.

Forordningen gælder endeligt i modsætning til databeskyttelsesdirektivet umiddelbart i de enkelte EU-lande og skal således ikke implementeres nationalt, hvilket sikrer ensartethed. Det kan således have været et problem, at databeskyttelsesdirektivet fra 1995 er blevet implementeret forskelligt i de enkelte medlemslande.

Styrkelse af de registreredes rettigheder

I forslagets art. 17 introduceres en "Ret til at blive glemt". Det er retten til at få slettet data, der bliver opbevaret enten hos den dataansvarlige eller på internettet.

Herudover skal en registreret have mulighed for at flytte sine egne data fra en onlinetjeneste til en anden, f.eks. mellem Facebook, Google+ og Twitter (dvs. således en "Ret til dataportabilitet" i forslagets art. 18).

Endelig skal den registrerede have ret til af den registeransvarlige at få en kopi af oplysninger, der er genstand for behandling, i et almindeligt anvendt elektronisk og struktureret format, som den registrerede kan anvende senere.

Underretningspligt ved brud på persondatasikkerheden

Yderligere indføres i artikel 31 en underretningspligt til tilsynsmyndigheden i forbindelse med brud for persondatasikkerheden, hvilket allerede kendes inden for telesektoren, hvor Erhvervsstyrelsen (tidligere IT- og Telestyrelsen) skal underrettes. Forpligtelsen i artikel 31 er baseret på underretningen af brud på persondatasikkerheden i artikel 4, stk. 3, i e-databeskyttelsesdirektivet. Underretningen skal foretages uden unødig for-

sinkelse og om muligt senest 24 timer efter, at den dataansvarlige er blevet bekendt med bruddet på persondatasikkerheden.

Endelig skal den registrerede efter artikel 32 i forslaget have meddelelse om sikkerhedsbruddet, når der er risiko for, at beskyttelsen af personoplysninger eller privatlivets fred vil blive krænket. Dette kan eksempelvis være tilfældet ved hackerangreb af et IT-system, hvor der er forekommet beskadigelse eller kompromittering af deri indeholdte personfølsomme data.

Skærpede krav til samtykke
Der indføres ligeledes skærpede krav til samtykke fra en registreret, hvorefter et samtykke ikke længere vil kunne bruges som behandlingsgrundlag, såfremt der er væsentlig ubalance mellem den registrerede og den dataansvarlige, f.eks. når der eksisterer et afhængighedsforhold. Det vil særligt kunne være tilfældet i forbindelse med samtykke afgivet i et ansættelsesforhold.

Med hensyn til personoplysninger for børn under 13 år skal der indhentes samtykke fra forældre eller værge i forbindelse med tilbud om informationssamfundstjenester.

I henhold til forslagets art. 7 skal et samtykke gives udtrykkeligt, og det må antages ikke at være tilstrækkeligt, at det sker i forbindelse med generelle vilkår og betingelser, da et samtykke skal være tydeligt adskilt fra eventuel anden tekst og andre forhold (eksplicit opt-in-samtykke).

Skærpelse af den registreringsansvarliges ansvar og øget selvregulering
Den registreringsansvarlige vil blive forpligtet til at begrænse sin behandling af personoplysninger til et absolut minimum og skal i den forstand overholde proportionalitetsprincippet, idet behandling kun må ske, hvis formålet ikke kan opnås ved mindre indgribende midler.

Der bliver ligeledes stillet krav om, at virksomheder skal udarbejde og implementere procedurer for behandlingen af persondata. Virksomheder med mere end 250 ansatte har pligt til at ansætte en databeskyttelsesansvarlig (DPO), der skal sikre, at virksomheden overholder reglerne i direktivet.

Virksomheder, der ønsker at overføre data til tredjelande, der ikke tilbyder samme beskyttelsesniveau som inden for EU, får mulighed for, på visse betingelser, at overføre data til disse lande, når overførslen er nødvendig på baggrund af legitime interesser, f.eks. i koncernforhold eller ved outsourcing til databehandlere, f.eks. cloud-løsninger. Koncernforbundne virksomheder skal i den forbindelse nemmere kunne indføre de så-

kaldte "Binding Corporate Rules", som regulerer overførslen mellem koncernselskaber. Blandt andet vil disse fremover kun skulle godkendes af myndighederne i ét EU-land.

Skærpelse af bødeniveauet
Forslaget vil indføre markant større bøder for overtrædelse af persondatareglerne. Der lægges således op til, at bøderne fremover skal udgøre mellem EUR 250.000 og 1 mio. alt efter karakteren af overtrædelsen.

Alternativt, når der er tale om virksomheder, kan der alt efter karakteren af overtrædelsen opkræves op til 2 % af virksomhedens årlige globale omsætning for overtrædelse af persondatareglerne. Forslagets artikel 79 oplister og rubricerer grovheden af en række overtrædelser, f.eks. fejlagtig opkrævning af gebyr for oplysninger til registrerede, utilstrækkelig ajourføring af oplysninger, manglende udlevering/overførsel af registreredes oplysninger, manglende eller ikke-rettidig anmeldelse af brud på persondatasikkerheden, manglende udpegelse af en databeskyttelsesansvarlig, uberettiget gennemførelse af videregivelse af personoplysninger til et tredjeland osv.

Op til 1 % af virksomhedens årlige globale omsætning gælder ved f.eks. overtrædelse af reglerne vedrørende indsamling af oplysninger. Op til 2 % af virksomhedens årlige globale omsætning gælder ved mere alvorlige overtrædelser, f.eks. behandling af oplysninger uden hjemmel eller uden samtykke fra den registrerede.

Betydning for nuværende behandling af persondata
Såfremt forslaget til forordningen accepteres i sin nuværende form, vil ændringerne pålægge erhvervsdrivende vidtgående forpligtelser ved deres behandling af persondataoplysninger samt betydeligt større sanktioner. Dette bringer persondata op på en virksomheds ledelsesniveau og er ikke blot udtryk for generel compliance.

Formålet med disse forpligtelser er ifølge Kommissionen at tilgodese de europæiske borgere og virksomheder. I stedet for at der som på nuværende tidspunkt er 27 nationale love bundet i databeskyttelsesdirektivet, vil der kun være én lov (dvs. forordning) og én tilsynsmyndighed, der regulerer alle forhold. For virksomhederne er det meningen, at dette skal lette den administrative byrde ved udveksling af oplysninger mod, at deres ansvar er større for behandlingen af oplysningerne. For borgerne betyder det, at rettighederne er ens for alle EU-borgere.

Brugere af sociale netværk og lignende vil som udgangspunkt få mulighed for at få deres data slettet fuldstændig, f.eks. når en konto lukkes. Behovet for videregående regulering er blevet nødvendigt, da det er 17 år siden, at de nuværende regler blev vedtaget.

Kommissionens forslag forholder sig ikke til, hvad "Retten til at blive glemt" vil betyde i forhold til journalistiske eller historiske oplysninger.

Næste skridt

Kommissionens forslag sendes nu videre til Europa-Parlamentet og Ministerrådet til drøftelser, hvilke må antages at føre til ændringer i forslaget. Såfremt forslaget vedtages, er der lagt op til, at forordningen vil træde i kraft to år efter endelig vedtagelse.

Inden for de næste par år må det antages, at forslaget i en revideret udgave vil blive gennemført baseret på de overordnede generelle punkter nævnt ovenfor. 2012 vil antageligt blive et afgørende år for virksomheder og andre aktører til at influere udkastet til forordningen.

Virksomheder bør allerede nu begynde at tænke indholdet af forslaget ind i virksomhedens forskellige systemer og processer til behandling af personoplysninger, f.eks. ved indkøb og opbygning af IT-systemer og tilrettelæggelse af forskellige administrative processer, da en omstilling af virksomhedens systemer og processer i forhold til de nye regler ikke kan ske fra den ene dag til den anden.

Hvis du har spørgsmål eller ønsker yderligere information om ovenstående, er du velkommen til at kontakte partner Nicolai Hesgaard (nhe@mwblaw.dk), advokat Henrik Syskind Pedersen (hsp@mwblaw.dk), eller advokatfuldmægtig Maria Thomsen (mth@mwblaw.dk).

Ovenstående er ikke juridisk rådgivning, og Moalem Weitemeyer Bendtsen indestår ikke for, at indholdet af ovenstående er korrekt. Moalem Weitemeyer Bendtsen har med ovenstående ikke påtaget sig ansvar af nogen art som konsekvens af en læsers benyttelse af ovenstående.