BRUD PÅ PERSONDATASIKKERHEDEN:

TYPISKE FEJL OG BØDENIVEAU

Datatilsynet oplyste i april 2019, at der stadig bliver anmeldt et højt antal sikkerhedsbrud godt 11 måneder efter, at databeskyttelsesforordningen trådte i kraft. Vi ser nærmere på de typesituationer, der forårsager et sikkerhedsbrud, hvordan disse kan undgås, sanktionsmuligheder og det kommende bødeniveau.

Datatilsynet har siden 25. maj 2018, hvor databeskyttelsesforordningen har skullet anvendes, og til og med 31. marts 2019 modtaget 4.301 anmeldelser om brud på persondatasikkerheden – sikkerhedsbrud. Omkring halvdelen af anmeldelserne kommer fra det offentlige, og mere end en fjerdedel kommer specifikt fra kommunerne.[1]

SANKTIONSMULIGHEDER

Som dataansvarlig er man som udgangspunkt forpligtiget til at anmelde et sikkerhedsbrud til Datatilsynet. Anmeldelsen skal ske uden unødig forsinkelse og om muligt senest 72 timer efter, at den dataansvarlige er blevet bekendt med bruddet. Hvis sikkerhedsbruddet sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, skal den dataansvarlige også underrette de personer, der har været berørt af sikkerhedsbruddet.

Datatilsynet har oplyst, at tilsynet er af den opfattelse, at sikkerhedsbrud, der udsætter fysiske personers rettigheder for risiko, generelt vil have karakter af forhold, som vil give anledning til – som minimum – kritik fra tilsynet.

Hvis sikkerhedsbruddet derimod fremstår som en afgrænset og enkeltstående hændelse med en ringe risiko for de registreredes rettigheder, og hvor den dataansvarliges foranstaltninger i forlængelse af bruddet vurderes som umiddelbart tilstrækkelige i forhold til beskyttelsen af de registreredes rettigheder, har Datatilsynet angivet, at tilsynet normalt vil afslutte sagen uden at udtale egentlig kritik. Dog vil sagen kunne genoptages ved nye oplysninger eller nye anmeldelser om sikkerhedsbrud fra den dataansvarlige. Pr. 31. marts 2019 har Datatilsynet afsluttet 1.555 sager alene med et brev til den dataansvarlige.

Hertil kommer, at den dataansvarlige kan blive mødt med en bøde.

Yderligere risikerer den dataansvarlige at blive mødt af krav om erstatning eller tortgodtgørelse fra de berørte personer, eventuelt i et såkaldt gruppesøgsmål, hvor flere personer går sammen om at søge økonomisk kompensation.

HVAD ER SIKKERHEDSBRUD, OG HVORNÅR SKER DE TYPISK?

Et sikkerhedsbrud er en hændelse, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse eller adgang til personoplysninger, der bliver behandlet.

Størstedelen af de brud, som Datatilsynet får anmeldt, har følgende karakter:

1. Personoplysningerne bliver sendt til den forkerte modtager

Ifølge Datatilsynet er mere end 2/3 af de anmeldte sikkerhedsbrud forårsaget af, at personoplysninger er blevet sendt til den "forkerte" modtager, oftest grundet en menneskelig fejl. Det er især e-mails eller almindelig brevpost, hvor modtageren eller adressen er blevet angivet forkert, eller hvor adressen ikke er blevet opdateret ved flytning, og brevet ved en fejl er blevet åbnet af en anden person.

Som dataansvarlig kan du for at imødekomme disse fejl med fordel fastsætte en række tekniske og organisatoriske sikkerhedsforanstaltninger. Datatilsynet nævner som eksempler på foranstaltninger at udarbejde procedurer for korrekt gennemførelse af de arbejdsopgaver, der indebærer behandling af personoplysninger, slå funktionen for autoudførelse af e-mailadresser fra eller undgå standardbreve, der bliver flettet til mange modtagere, ligesom bcc og ikke cc benyttes ved afsendelse af mails til flere modtagere.

2. Tyveri af udstyr eller dokumenter

En forholdsvis stor gruppe af sikkerhedsbrud relaterer sig til tyveri eller tab af udstyr eller dokumenter, der indeholder personoplysninger. Det kan være en taske, der indeholder en række dokumenter, der er blevet glemt i toget, eller en bærbar computer eller telefon, der er blevet stjålet.

Datatilsynet har flere gange understreget, at fysiske enheder, og især de enheder, der hyppigt er udsat for tyveri eller let mistes under transport, som udgangspunkt slet ikke skal indeholde personoplysninger, og i det omfang den dataansvarlige har vurderet, at de kan indeholde sådanne oplysninger, skal indholdet være krypteret på en sådan måde, at ingen uvedkommende kan læse de pågældende oplysninger, hvis enheden mistes.

3. Manglende fortrolighed af personoplysningerne

En tredje gruppe af sikkerhedsbrud vedrører de situationer, hvor en personlig fejl medfører, at oplysningerne ikke bliver underlagt den fortrolighed, som den dataansvarlige egentlig har vurderet nødvendig for behandlingen, eksempelvis e-mails, der efter intern instruks skulle sendes krypteret, men som alligevel bliver sendt ukrypteret.

Disse situationer kan være svære for den dataansvarlige at gardere sig imod, men sådanne fejl vil typisk kunne forhindres eller minimeres ved organisatoriske sikkerhedsforanstaltninger, herunder uddannelse og procedurer, som sætter fokus på at sørge for det rette sikkerhedsniveau ved forsendelser.

4. Phishing, malware og hacking

Brud på persondatasikkerheden, der skyldes udefrakommende påvirkning såsom phishing, malware eller hacking, udgør mindre end 5 % af de samlede anmeldelser.

Den dataansvarlige bør dog alligevel instruere sin IT-afdeling og eventuelle databehandlere om at foretage konkrete tekniske og organisatoriske sikkerhedsforanstaltninger imod sådanne angreb, herunder foretage løbende opdateringer af alle relevante systemer samt altid at have en rigtigt konfigureret firewall.

BØDENIVEAUET

Der findes endnu ikke en generel guide for, hvad det "koster" i bøde at overtræde databeskyttelsesforordningen. I Europa er der på nuværende tidspunkt givet bøder på mellem EUR 5.000 og EUR 50 mio., eksempelvis til den norske kommune Bergen, der i januar modtog en bøde på NOK 1,6 mio. fra det norske datatilsyn for overtrædelse af databeskyttelsesforordningen.

Det store spænd i bødestørrelserne er udtryk for, at bødeniveauet beror på en konkret vurdering.

Med forordningen har man dog lagt op til, at bødeniveauet gerne skal ensartes i Europa. Det hollandske datatilsyn har i denne forbindelse udgivet sine retningslinjer for bødeniveauet. Retningslinjerne indeholder forskellige grupperinger af overtrædelser, hvor der angives mellem tre og fire "bødekategorier" med en nærmere angivet "bødebåndbredde" og en grundbøde.

De hollandske retningslinjer indeholder også en liste over faktorer, som er relevante i forhold til vurderingen af alvoren af en overtrædelse og bødens størrelse. Af listen fremgår, at der blandt andet lægges vægt på omfanget af overtrædelsen, herunder antallet af berørte personer, de foranstaltninger, der er blevet truffet for at begrænse de registreredes tab, samarbejdet med tilsynsmyndigheden, og om der er sket lignende brud tidligere.

Det er endnu uvist, i hvilket omfang det danske datatilsyn vil følge de hollandske retningslinjer, men som nævnt må der forventes en vis ensartethed i det europæiske bødeniveau.

DATATILSYNETS FØRSTE POLITIANMELDELSE

Datatilsynet politianmeldte 18. marts 2019 Taxa 4x35 og indstillede samtidig selskabet til en bøde på 1,2 mio. kr. Det er den første bøde, som Datatilsynet har indstillet til efter forordningens bestemmelser.

Datatilsynet fandt i denne sag, at Taxa 4x35 ikke overholdt flere grundlæggende principper i forordningen. Fx opbevarede Taxa 4x35 personoplysninger i tre år længere end nødvendigt, bl.a. fordi selskabets it-system gjorde det besværligt at efterleve reglerne i forordningen. Denne indstilling indikerer meget klart, at bødeniveauet for overtrædelse af databeskyttelsesforordningen også i Danmark for fremtiden vil få et markant højere niveau end efter reglerne, som var gældende før 25. maj 2018. Dette var også forventningen og formålet med de nye regler i databeskyttelsesforordningen ■

1 Se Datatilsynets opgørelse for perioden 25. maj - 31. december 2018 og opgørelsen for første kvartal af 2019.

Mads Nygaard Madsen
Advokat, partner
mnm@horten.dk

Charlotte Kunckel
Specialistadvokat
cku@horten.dk

Christoffer Alsted Skafte
Advokatfuldmægtig
chs@horten.dk