FCG - YOUR INNOVATIVE PARTNER IN RISK MANAGEMENT, FINANCIAL REGULATION AND GOVERNANCE

FCG INSIGHT

Ny GDPR vejledning fra Datatilsynet;

Håndtering af brud på datasikkerheden

Håndtering af brud på persondatasikkerheden

Ny vejledning fra Datatilsynet

Den 28. februar 2018 offentliggjorde Datatilsynet sin seneste vejledning til den kommende Persondataforordning (GDPR) om emnet *"håndtering af brud på persondatasikkerheden"*. Den nye vejledning er nummer otte af i alt tretten vejledninger, som Datatilsynet udarbejder om forståelsen og anvendelsen af GDPR, som træder i kraft den 25. maj 2018. Vejledningen supplerer en tilsvarende vejledning fra den såkaldte "art. 29-gruppe", som er et rådgivende organ nedsat i medfør af det nugældende persondatadirektiv fra 1995 (art. 29-gruppen erstattes ifm. ikrafttræden af GDPR af Databeskyttelsesrådet).

Vejledningen vedrører forordningens art. 33, som fastslår, at anmeldelse af brud på persondatasikkerheden skal ske uden unødig forsinkelse og om muligt senest 72 timer efter, at den dataansvarlige er blevet bekendt med bruddet.

Anmeldelse til Datatilsynet

Et brud på persondatasikkerheden er i GDPR defineret som *"et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet"*. Hacking og ubeføjet videregivelse er således klassiske eksempler på sikkerhedsbrud.

Som udgangspunkt skal alle brud på persondatasikkerheden anmeldes til Datatilsynet, medmindre det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, fx på grund af den dataansvarliges sikkerhedsforanstaltninger. Hvorvidt en sådan risiko foreligger eller ej, skal i hvert enkelt tilfælde vurderes af den dataansvarlige. Anmeldelsen skal, i Danmark, gives til Datatilsynet, som arbejder på at etablere én fælles digital løsning for sådanne anmeldelser. Denne vil blive placeret på virk.dk.

Anmeldelse af brud på datasikkerheden skal ske uden unødig forsinkelse, og om muligt senest 72 timer efter bruddet. Denne frist igangsættes på det tidspunkt, hvor den dataansvarlige er *bekendt med*, at der er sket et brud på persondatasikkerheden. En formodning er derfor ikke tilstrækkelig. Derimod bør en formodning føre til den dataansvarliges undersøgelse af sagen, for at be- eller afkræfte formodningen. 72 timers-fristen er imidlertid ikke absolut, og det tillades, at anmeldelse kan ske efter de 72 timer, såfremt den dataansvarlige kan redegøre for de særlige grunde, der umuliggjorde en anmeldelse inden for tidsfristen.

Det er som udgangspunkt den dataansvarlige, som foretager anmeldelse, men denne kan (og bør) bemyndige en eller flere medarbejdere i organisationen til at foretage anmeldelsen på dennes vegne. Derudover kan databehandleren være bemyndiget til at foretage anmeldelse på vegne af den dataansvarlige, hvilket bør fremgå af databehandleraftalen, men det overordnede juridiske ansvar for den rettidige anmeldelse vil forblive hos den dataansvarlige.

Databehandleren er forpligtet til uden unødig forsinkelse at underrette den dataansvarlige om et brud, herunder en formodning om et brud. Art. 29-gruppen anbefaler i sin vejledning om brud på datasikkerheden (WB250), at databehandlerens underretning

foretages straks. Forpligtelsen for databehandlerens underretning, bør tillige fremgå af databehandleraftalen.

Underretning til den registrerede

Foruden ovenstående anmeldelse er den dataansvarlige forpligtet til at underrette den registrerede. En sådan underretning skal gives, når et brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder. Ved denne vurdering må risikoens omfang bl.a. lægges til grund - jo mere alvorlige konsekvenser bruddet kan medføre, jo større vil risikoen være for de berørte personer. Underretningen bør foretages, så snart det med rimelighed er muligt.

Såvel den dataansvarlige og databehandleren kan underrette den registrerede, såfremt den dataansvarlige har uddelegeret opgaven til databehandleren. Dette kræver en bemyndigelse hertil, og skal fremgå af databehandleraftalen.

Dokumentation og procedurer

Alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet, dets virkninger og de trufne afhjælpende foranstaltninger, skal dokumenteres. Det er uden betydning for dokumentationspligten, om bruddet har været af en sådan karakter, at den dataansvarlige har været forpligtet til at underrette Datatilsynet eller ej. Art. 29-gruppen anbefaler, at den dataansvarlige tillige sørger for at dokumentere sine begrundelser for alle væsentlige beslutninger, der træffes som følge af bruddet – i særdeleshed, hvis den dataansvarlige har vurderet, at bruddet ikke skal anmeldes til Datatilsynet. Der stilles ikke specifikke formkrav til dokumentationsforpligtelsen, og den dataansvarlige kan derfor selv beslutte, hvordan oplysningerne skal indsamles, og hvordan de skal præsenteres.

Foruden anmeldelse til Datatilsynet er der i medfør af anden lovgivning krav om anmeldelse til andre myndigheder, herunder til Finanstilsynet. Finanstilsynet forventer at blive orienteret om væsentlige it-hændelser hos finansielle virksomheder og fælles datacentraler. Derudover stiller lov om betalinger krav om, at udbydere af betalingstjenester snarest muligt skal underrette Finanstilsynet om større drifts- og sikkerhedshændelser.

Det er afgørende for at sikre en effektiv og ensartet efterlevelse af forpligtelsen til at anmelde brud på persondatasikkerheden og til at underrette de registrerede, at der udarbejdes interne procedurer for håndtering af sikkerhedshændelser i organisationen. Sådanne procedurer kan, jf. ISO-standarden (ISO 27001), eksempelvis indeholde bestemmelser om rapportering og vurdering af hændelser, herunder ansvarsfordeling. Endelig bør den dataansvarlige (og evt. databehandleren) overveje, hvilke tekniske og organisatoriske foranstaltninger der kan indføres i organisationen for at sikre, at brud på persondatasikkerheden opdages og håndteres korrekt.

Kontaktoplysninger

Line Poulsen, Associate
Line.Poulsen@fcg.dk
+45 53 73 69 61

Som finansielle konsulenter er vores ambition at se nye muligheder og finde innovative løsninger. Det er i vores DNA at være på forkant inden for vores specialistområder og udfordre vores kunder til at tænke nyt. Vi arbejder langsigtet i vores partnerskaber og er på den måde understøttende gennem hele behovskæden, helt fra analyser og fortolkning til implementering og forvaltning.

FCG har sit udgangspunkt i den danske og internationale implementering af finansielle regler. Vi er specialister inden for risikostyring og kapitalhåndtering samt compliance og governance. Vores målsætning er, at vores kunder har et godt ry, at de opfylder kravene i lovgivningen, og at de får maksimalt udbytte af samarbejdet med FCG.

FCG er, med et stærkt fokus indenfor business management, unikke i Norden når det gælder etablering af strategier og effektive processer, som muliggør at vores kunder kan opbygge fremtidens virksomhed med de rigtige kunder, produkter, priser og kanaler.

FCG-koncernen har kontorer i Danmark, Sverige og Norge, hvor der samlet findes omkring 150 eksperter i jura, økonomi, regnskab, matematik og aktuarservices. FCG har kunder i alle segmenter og størrelser, der er under tilsyn af Finanstilsynet, men vi hjælper også virksomheder i andre brancher, der møder regulering eller som kan se fordelene ved best practice/corporate management samt håndtering af kredit-, finans- og risikospørgsmål.

FCG. +45 70 20 69 60. info@fcg.dk. Amaliegade 5C, 3. Sal DK-1256 København K. **fcg.dk**