DANSK ERHVERV
Børsen
1217 København K

www.danskerhverv.dk
info@danskerhverv.dk
T. + 45 3374 6000

Justitsministeriet
Att.: Mikkel Reenberg

Den 07.10.2020

National evaluering af databeskyttelsesreglerne

Dansk Erhverv og IT-Branchen sætter stor pris på, at Justitsministeriet har taget initiativ til en evaluering af GDPR- reglerne. Vi går ud fra, at processen alene har til formål at afdække, hvorvidt visse procedurer kan gøres enklere etc. indenfor forordningens rammer, men selv om råderummet derved bliver begrænset, så er initiativet meget tiltrængt!

Under henvisning til Justitsministeriets skrivelse af 07.04.d.å. skal vi hermed skitsere og kommentere nogle af de væsentligste problemstillinger virksomhederne oplever i deres daglige virke med GDPR.

1. Dataansvarlig eller databehandler

Problemstillingen omkring, hvornår man er det ene eller det andet, er et af de emner vi har drøftet mest med vores medlemmer i de sidste to år. Det er i praksis meget vanskeligt at slå fast, hvornår man er det ene eller andet. Virksomheder har vanskeligt ved at forstå, hvorfor eksempelvis PostNord ikke er databehandler, når de bringer posten ud, mens en tjeneste, der sender e-mails ud, er. Dette er særligt relevant ved it-leverandører, hvor leverandørens opgave ikke er at behandle persondata, men hvor leverandøren har adgang til systemet, f.eks. i forbindelse med teknisk support.
Det er endvidere et emne, der medfører mange konflikter i kunde-leverandørforholdet idet mange dataansvarlige ikke har lyst til at indgå databehandleraftaler på grund af de administrative konsekvenser det medfører. Der skal udarbejdes instrukser, føres tilsyn med både databehandlere og underdatabehandlere osv. Situationen er derfor mange gange den, at en virksomhed- for nøjagtige samme tjeneste- vurderes som værende databehandler af den ene kunde, mens den anden kunde mener, at pågældende leverandør er dataansvarlig.

Der bør derfor ske en udbygning af Datatilsynets vejledning i samarbejde med relevante organisationer, og vejledningen skal bringes i overensstemmelse med vejledningen fra EDPB. Vejledningen kunne suppleres med en FAQ på Datatilsynets hjemmeside vedrørende dette emne.

2. Eksport af data til 3.lande (udfordringer ved cloud)

Efter Shrems II sagen, er det blevet uhyre vanskeligt at eksportere data til 3.lande, idet det nu er uomtvisteligt, at den dataansvarlige skal forholde sig til de 4 europæiske garantier. Det er ikke længere nok at gøre brug af EU´s standardblanket, idet standardblanketten skal suppleres med yderligere overvejelser og undersøgelser, hvis rækkevidde for øjeblikket er uklar. Dette er i realiteten en stor udfordring i forhold til anvendelsen af cloudløsninger både i det private, men i særdeleshed i offentlig regi.
De fire essentielle garantier er en tung og besværlig måde at skabe et overførselsgrundlag. Der er brug for alternativer meget hurtigt, og Justitsministeriet skal sørge for, at der presses på for at finde en løsning i EU-regi.

3. Datatilsynets rolle

a) Vejledninger og værktøjer

Det er glædeligt, at Datatilsynet i sin just offentliggjorte strategi oplyser at ville opprioritere vejledningsindsatsen.
Set i bakspejlet burde Datatilsynet være kommet tidligere på banen med vejledninger og værktøjer. Mange af vejledningerne var ikke færdige før den 25.05.2018, men mange af vejledningerne har dog fået et tilfredsstillende niveau, og kom til verden med input fra erhvervslivet. Denne tilgang bør klart bibeholdes, når vejledningerne skal opdateres.

En ting er gode vejledninger, en anden ting er gode eksempler. Vi mener, at Datatilsynet via detaljerede eksempler bør belyse, hvordan virksomhederne lever op til reglerne. Datatilsynet mangler f.eks. at beskrive nærmere, hvad der helt præcist skal til, for at man som mindre virksomhed overholder reglerne: Hvordan skal et håndværkerfirma eller en boligorganisation dokumentere, at de overholder reglerne? Det kunne beskrives i form af en fiktiv case fra A-Z. Og hvad med en praktisk vejledning til, hvordan man i detaljer opfylder kravene, når man ønsker at optage en tlf samtale til uddannelsesformål?
Man kan naturligvis ikke beskrive, hvordan alle mulige virksomheder præcist skal leve op til reglerne, men 4-5 fiktive cases ville hjælpe på forståelsen.

Sluttelig savnes i tillæg til de gode eksempler brugbare tjeklister.

b) Bindende forhåndsbesked

Vi efterspørger også muligheden for at Datatilsynet kan give bindende forhåndsbesked til konkrete databehandlinger. Lige nu skal der tilnærmelsesvis være et kontrolbesøg for at virksomheden kan få et bindende svar på om de overholder reglerne.
Det er endvidere afgørende at Datatilsynet kan svare hurtigt på henvendelser, da længere usikkerhed vil medføre forsinkelser og tilbageholdenhed i relation til nye initiativer som eksempelvis AI.

4. Minimumsgrænse for simple databrud

Virksomheder er tit i tvivl om, hvorvidt et givent brud skal anmeldes.

Det ville være ønskeligt, hvis Datatilsynet i videre omfang kunne klarlægge de situationer, hvor en anmeldelse af et brud på persondatasikkerheden, **ikke** skal anmeldes. Det følger af Datatilsynets vejledning, at et brud ikke skal anmeldes, hvis det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, men vejledningen siger ikke ret meget om de parametre, der indgår denne vurdering. Datatilsynet bedes via flere eksempler præcisere, hvordan den Dataansvarlige kan løfte bevisbyrden, heraf skitsere hvilke omstændigheder, som typisk skal være til stede for at en risiko er usandsynlig. Datatilsynet bedes angive, hvornår vurderingen skal foretages, og om der altid skal være foretaget en vurdering, før en anmeldelse sker til Datatilsynet.

I den reviderede vejledning bør det også præciseres, at den dataansvarlige er forpligtet til at meddele databehandleren, hvem der skal modtage oplysning om databrud, og at denne oplysning jævnligt opdateres.

Kan der evt. etableres en mere håndgribelig bagatelgrænse for sikkerhedsbrud?

5. I hvilket omfang gælder reglerne for de personer, der agerer på vegne af en virksomhed

De fleste virksomheder, der handler BtB har ikke forbrugerdata i deres CRM-system. De typiske persondata, som disse virksomheder håndterer – når man ser bort fra data om deres egne medarbejdere – er telefonnumre og e-mailadresser på kontaktpersoner hos virksomhedens kunder eller leverandører. Datatilsynet har ved flere lejligheder udtalt, at det ikke er den slags persondata man går efter, men det ville overordentlig vigtigt, hvis der kunne komme klarhed omkring, hvorvidt denne type persondata kan håndteres anderledes end

6. Kontrol af databehandlere

Virksomheder føler sig usikre omkring, hvorvidt de overholder reglerne. Jf. punkt 3 kunne det også her være formålstjenligt, hvis der var et eksempel på en konkret case, der opfylder kravene, og hvor kontrollen ikke består af en 3.parts erklæring, men af virksomhedens eget spørgeskema og/eller et fysisk besøg hos databehandleren. Der efterlyses værktøjer til, hvordan man kunne gribe det an.

Det er vigtigt at sikre, at kontrollen og dokumentationskravene er proportional(e) i forhold til den databehandling der sker, og at dette aspekt beskrives tydeligere og igen ved illustrative eksempler.

7. Fastlæggelse af rollefordeling, når erhvervslivet er leverandør til det offentlige

Vurderingen af, om leverandøren af en given ydelse enten er dataansvarlig eller databehandler varierer fa kommune til kommune, selv om der er tale om den samme leverance.
Det bør overvejes, hvorvidt rollefordelingen skal fastsættes ved lov. Der er i dag forskellige tolkninger på tværs af myndigheder og samme ydelser giver fx 98 forskellige aftaler i 98 kommuner.
Alternativt kan der oprettes et katalog over service, tjeneste og vareydelser, hvor der redegøres for, hvilken rolle kommunen og dens leverandør indtager i relation til datahåndtering.

8. Håndtering af mailsystemer

Mens mange virksomheder kan forstå, at der skal slettes data i CRM og ERP systemer m.fl. når formålet er udtømt, hersker der usikkerhed omkring, hvordan Datatilsynet ser på de persondata, der er indeholdt i mailsystemer som outlook etc. Disse ustrukturerede data rejser forskellige problemstillinger i relation til sletning, indsigtsret osv. og der er behov for en vejledning i håndteringen af disse systemer.

9. Anonymisering af data

Der er usikkerhed omkring anonymisering af data. Hvornår er data anonyme og derfor ikke persondata – fx syntetiske data.

Med venlig hilsen

Sven Petersen
Erhvervsjuridisk fagchef
Dansk Erhverv

Martin Jensen Buch
Chefkonsulent
IT-Branchen