

Forsikring & Pensions hørings svar til Datatilsynet vedr. vejledning om tredjelandsoverførsler

Forsikring & Pension takker Datatilsynet for muligheden for at kommentere på udkast til opdateret vejledning vedrørende overførsel af data til tredjelande.

Det er positivt at Datatilsynet tager initiativ til en opdatering af den eksisterende vejledning og derved også følger op på anbefalingerne fra Erhvervslivets EU- og Regelforum, som har efterlyst mere lavpraktisk og uddybende vejledning, som bl.a. bedre afgrænser selve overførselsbegrebet og introducerer flere praktiske eksempler til brug for efterlevelsen af forordningens krav i forbindelse med overførsel af data til tredjelande. Det er umiddelbart vurderingen, at Datatilsynets udkast omfatter gode og relevante eksempler.

Det giver dog også anledning til en vis forvirring at vejledningen kommer nu, idet de fleste interessenter i høj grad har rettet opmærksomheden mod Det Europæiske Databeskyttelsesråd (EDPBs) og deres endelige guidelines i relation til tredjelandsoverførsler. EDPBs guidelines, der efter vores oplysninger ventes omkring 15. juni 2021, formodes at skabe større klarhed og bringe både dataansvarlige og databehandlere ud af den betydelige usikkerhed omkring dataansvaret, der har hersket siden EU-Domstolens afgørelse i Schrems II og som har begrænset en del forretningsaktiviteter. Det er selvsagt afgørende, at Datatilsynets vejledning harmonerer med udmeldingerne fra EDPB og er klart afgrænset i forhold hertil, hvorfor vi gerne havde set at Datatilsynet havde ventet med opdateringen af den nationale vejledning om tredjelandsoverførsler til efter de ventede guidelines fra EDPB.

Forsikring & Pension har følgende konkrete bemærkninger til udkastet:

Bemærkninger til afsnit 2 om hvornår der er tale om en overførsel?

Forsikring & Pension finder det relevant og brugbart med vejledningens praktiske eksempler, her særligt eksempel 1-6. Dog er der behov for visse præciseringer:

07.06.2021

Forsikring & Pension
Philip Heymans Allé 1
2900 Hellerup
Tlf.: 41 91 91 91
fp@forsikringogpension.dk
www.forsikringogpension.dk

Karen Gjølbø
Chefkonsulent
Dir. 41919045
kgj@forsikringogpension.dk

Sagsnr. GES-2021-00221
DokID 426321

(Eksempel 4) Forsikring & Pension hilser udmeldingen om, at der ikke er tale om en tredjelandsoverførsel, når medarbejdere i udlandet logger på virksomhedsnetværk via VPN-forbindelse, velkomment. Det bør dog her præciseres, at dette ikke blot gælder i forbindelse med forretningsrejser, som anført, men i alle tilfælde, hvor en medarbejder logger på via VPN fra et tredjeland.

(Eksempel 5) Det er ikke umiddelbart klart, hvorfor der i forhold til spørgsmålet om overførsel eller ej er forskel på situationen, hvor data holdes indenfor en juridisk enhed mellem et selskab og en filial, og så situationen, hvor data udveksles mellem et selskab og dets datterselskab, i det omfang data sendes til og behandles i et tredjeland?

Samtidig giver dette eksempel anledning til yderligere præcisering i forhold til andre konstellationer med udveksling af data med tredjeparter, f.eks. konsulenter på kontrakt med en dataansvarlig, der arbejder på et kontor i et tredjeland. Spørgsmålet er hvorvidt der her er tale om tredjelandsoverførsler på lige fod med eksempel 5 hvis f.eks. følgende forudsætninger er til stede:

1. Konsulenten har kontrakt med en dataansvarlig og alene udfører aktiviteter under den dataansvarliges instruks og ikke til egne formål?
2. Konsulenten alene arbejder i den dataansvarliges bygninger?
3. Konsulenten har forpligtet sig til tavshedspligt og er underlagt dataansvarliges retningslinjer for medarbejderens sikkerhedsadfærd?
4. Konsulenten har forpligtet sig til alene at arbejde i den dataansvarliges systemer via VDI-adgang og via computer udleveret af den dataansvarliges virksomhed?
5. Konsulenten kun får adgang til data i samme omfang som en ansat hos den dataansvarlige med tilsvarende opgaver?

I forlængelse heraf ville det være behjælpeligt, hvis Datatilsynet kunne medtage yderligere eksempler og præcisere hvorvidt der er tale om overførsel i følgende situationer:

1. Udveksling af data i forbindelse med kommunikation med kunder, der er bosat i et tredjeland?
2. Fremsendelse af sms med personoplysninger til en kunde med en dansk mobil, som tilfældigvis befinder sig i et usikkert tredjeland?
3. Fremsendelse af et brev med personoplysninger i e-boks eller til en kundes e-mail og kunden vælger at tilgå e-bos eller e-mail, mens vedkommende befinder sig i udlandet på rejse?

(Eksempel 6) Det er ligeledes positivt med en præcisering af dataansvaret i eksempel 6, der begrænser dette når data overføres i strid med databehandleraftalen. Det ville her tillige være hjælpsomt, hvis Datatilsynet kunne:

1. Uddybe med eksempler i forhold til hvad der er tilsigtede og utilsigtede overførsler, samt
2. forholde sig til betydningen af, at de store tech-giganter, som Microsoft, AWS, Salesforce etc. som standard ikke vil eller kan garantere, at data ikke overføres til tredjelande og således reelt ikke kan benyttes, på trods af i øvrigt høje sikkerhedsstandarder hos de pågældende selskaber.

Bemærkninger til afsnit 3 om behov for overførselsgrundlag (sikre og usikre tredjelande)?

Forsikring & Pension ønsker en præcisering af eksemplet omkring Rigsfællesskabet på side 12, herunder i forhold til Færøerne, hvad der skal forstås som "rigsmyndigheder" (gælder dette f.eks. det færøske skattevæsen, TAKS?) og i forhold til Grønland, om det er muligt at sige noget om, hvorvidt der er taget skridt henimod en tilstrækkelighedsafgørelse fra Kommissionen?

Bemærkninger til afsnit 4 om overførselsgrundlaget

(side 14) I forhold til Kommissionens standardkontrakter og teksten omkring standardkontrakter som del af en bredere kontrakt, foreslås præciseret – evt. i tilknytning til kommentarboksen om ny version af Kommissionens standardkontrakter - at det af EDPBs udkast til anbefalinger pkt. 56 følger, at tilføjelser af bestemmelser til standardkontrakterne om supplerende mitigerende tiltag ikke vil kræve godkendelse, så længe at de ikke er i modstrid med bestemmelserne i standardkontrakterne.

Bemærkninger til afsnit 5 om øvrige opmærksomhedspunkter

(side 18) Eksemplet vedrørende efterlevelse af oplysningsforpligtelsen er meget forsimplet og langt fra den virkelige verden i en stor organisation. Det vil være fint, om Datatilsynet også kunne komme med eksempler der afspejler, at der kan være tale om overførsel til flere lande, hos flere leverandører, hvor der sker løbende opdateringer af de lande, der overføres data til (selvfølgelig under behørig iagttagelse af kravet om tilstrækkelig databeskyttelse).

(side 19) Henvisningen til Schrems II-afgørelsen er centralt for en vejledning om tredjelandsoverførsler, men her er det tydeligt, at Datatilsynet bør afvente EDPBs endelige guidelines for at undgå uoverensstemmelser og yderligere usikkerhed omkring dataansvaret. Med Datatilsynets formuleringer fastholdes det urealistiske krav til dataansvarlige i forhold til at vurdere tredjelandets lovgivning, som forventes imødegået i en vis grad i EDBS endelige guidelines.

I afsnit 5 på siden fremhæver Datatilsynet, at dataeksportøren er forpligtet til at sikre sig at beskyttelsesniveauet i tredjelandet "essentielt" svarer til det som vi har i EU. "Essentielt" bør erstattes med "i det væsentlige". Dels mener Forsikring & Pension at ordlyden bør følge præambelbetragtningerne, jf. nr. 104 og Schrems II dommen, dels er det vores forståelse, at der er en sproglig forskel på de to formuleringer.

(side 20) I afsnit 4 henvises til EDPBs guidelines omkring supplerende foranstaltninger og det anføres at tekniske foranstaltninger altid vil være nødvendige og at organisatoriske og kontraktuelle foranstaltninger aldrig vil kunne stå alene. Dette synes umiddelbart at være en lidt vidtgående tolkning af EDPBs udkast til guidelines, se bl.a. pkt 48, hvoraf det fremgår at "contractual and organisational measures alone will generally not overcome access to personal data by public authorities of the third country. Det er dog ikke udelukket efter teksten.

Bemærkninger til afsnit 6 om overførsel i særlige situationer

Der er behov for en præcisering i vejledningen i forhold til kravet om, at overførsler efter undtagelsesbestemmelserne alene må være lejlighedsvis. Hvad ligger der nærmere heri? Forsikringsselskaber har hvad de ville betegne som lejlighedsvis overførsel af data til bl.a. de grønlandske og færøske skattemyndigheder, som ikke sker regelmæssigt eller hyppigt, men som dog gentages? Hvor meget skal der til for at noget ikke længere er lejlighedsvist?

(side 22-23) Det ville være ønskeligt, om der kunne gives flere eksempler på, hvornår noget skal betragtes som "nødvendigt" for opfyldelse af en kontrakt, herunder en uddybning af hvad der menes med "at der skal være en tæt og betydelig forbindelse" mellem overførslen af personoplysninger og kontraktens formål".

Bemærkninger til afsnit 1 om hvad der er personoplysninger

Indledningsvist kunne være anført, at Datatilsynet bør fastslå, om ikke her, så i anden vejledning, hvorvidt arbejdsmails og arbejdstelefonnummer er at opfatte som personoplysninger. Sådanne oplysninger udveksles i mange sammenhænge og sendes også gerne over grænser i forbindelse med bl.a. internationale konferencer, forskningsprojekter etc. Det vil i den forbindelse formentlig også kunne forekomme at oplysninger sendes i en mere lind strøm end blot lejlighedsvis overførsler. Det synes dog ikke helt proportionalt, hvis man her skulle kræve en omfattende vurdering af beskyttelsesniveauet i et givent tredjeland.

Forsikring & Pension står naturligvis til rådighed for eventuel uddybning af ovenstående bemærkninger.

Vi vil dog afslutningsvist gentage opfordringen til at afvente EDPBs endelige guidelines for færdiggørelse af nærværende vejledning for at sikre overensstemmelse og bedre klarhed mellem de to.

Med venlig hilsen

Karen Gjørbo