Ny vejledning vedrørende brugen af cloudservices

Databeskyttelsesreglerne fortæller ikke noget om, hvilke teknologier en organisation må bruge til at behandle personoplysninger, idet reglerne er teknologineutrale. Der er dog nogle teknologier, som giver anledning til flere udfordringer end andre.

I lyset af Schrems II-afgørelsen og de efterfølgende afgørelser fra det østrigske og det franske datatilsyn vedrørende brugen af Google Analytics har der været en del uvished omkring brugen af cloudservices. Derfor har Datatilsynet nu udgivet en ny vejledning, der har til formål at hjælpe organisationer, der benytter eller påtænker at benytte sig af cloudservice. Samtidig får udbydere af cloudservices mulighed for at læse, hvordan de kan levere ydelser i overensstemmelse med databeskyttelsesreglerne. Vejledningen findes også på engelsk.

VEJLEDNINGENS INDHOLD

Udover en udførlig gennemgang af de forskellige slags cloudservices man som organisation kan vælge imellem, indeholder vejledningen en gennemgang af de overvejelser, man bør gøre sig i forbindelse med valget af en cloudløsning samt en række praktiske anbefalinger.

KEND DINE SERVICES OG LEVERANDØRER

Det er et helt grundlæggende krav efter databeskyttelsesreglerne, at man som dataansvarlig har overblik over, hvilke personoplysninger der behandles, til hvilke formål de behandles, og hvordan de behandles. Dette er nødvendigt for, at man kan foretage de påkrævede risikovurderinger.

Vejledningen giver en række spørgsmål, der bør besvares i forbindelse med de påkrævede risikovurderinger af databeskyttelsen og sikkerhedsniveauet. Det er vigtigt at pointere, at disse risikovurderinger skal laves, uanset om man benytter sig af cloudleverandører eller ej, men at en sådan brug vil tilføje flere faktorer til risikovurderingerne.

Vejledningen angiver, at en dataansvarlig bør stille disse spørgsmål i forbindelse med risikovurderingen vedrørende databeskyttelse:

1. Behandler cloudleverandøren yderligere personoplysninger end de personoplysninger, som er overladt til cloudleverandøren? F.eks. metadata eller andre tjenestedata.
2. Behandler cloudleverandøren de personoplysninger, der er overdraget cloudleverandøren til egne formål? Hvis ja, skal der findes en hjemmel

Vejledningen angiver derudover, at den dataansvarlige bør fastslå leverandørens sikkerhedsniveau og vurdere, om dette sikkerhedsniveau er passende i forhold til sin risikovurdering.

Derudover oplister vejledningen en række spørgsmål, den dataansvarlige bør bruge ved screening af cloudleverandører, og der gives en uddybende forklaring vedrørende de vigtigste punkter.

TILSYN MED CLOUDLEVERANDØREN OG EVENTUELLE UNDERLEVERANDØRER

Datatilsynet uddyber også kravene til tilsynet med databehandlere og underdatabehandlere i forhold til cloudleverandører. Dette skal ske i tillæg til de krav, der findes til tilsynet med databehandlere, som man kan læse nærmere om i Datatilsynets vejledning om tilsyn med databehandlere.

I vejledningen fastslås det, at den dataansvarlige bør gennemgå revisionsrapport (hvor sådanne foreligger), men at det er nødvendigt at være opmærksom på, om revisionsrapporten vedrører de behandlingsaktiviteter, som cloudleverandøren foretager for den dataansvarlige.

Hvis der ikke foreligger relevante revisionsrapporter, skal den dataansvarlige sikre sig, at de er berettiget til at kræve en revision af behandlingsaktiviteterne.

OVERFØRSLER TIL TREDJELANDE, HERUNDER USA

Den nye vejledning understreger de tidligere udmeldinger fra Datatilsynet vedrørende overførsler til tredjelande og supplerende foranstaltninger.

Det mest væsentlige at være opmærksom på i forbindelse med brugen af cloudservices udenfor EU/EØS (tredjelande), er den Transfer Impact Assessment (TIA), der skal udarbejdes, og vurderingen af, om der skal indføres supplerende foranstaltninger. TIA-vurderingen er relativ ny og er indført på baggrund af Schrems II-afgørelsen. Vejledningen understreger blot, at man fortsat skal følge fremgangsmåden, som er fastsat i Datatilsynets "Vejledning om overførsel af personer til tredjelande" og anbefalingerne fra EDPB.

Vejledningen berør dog også den specielle udfordring, der er vedrørende overførsler af personoplysninger til USA, og som Schrems II og særligt de nye afgørelser fra Østrig og Frankrig vedrørende Google Analytics har givet anledning til.

Datatilsynet nævner, at der skal implementeres effektive supplerende tekniske foranstaltninger i de tilfælde, hvor en cloudleverandør i USA er omfattet af FISA 702, hvilket de som oftest er. Datatilsynet understreger dog, at hvis en sådan cloudleverandør har adgang til personoplysninger i klartekst, kan Datatilsynet på nuværende tidspunkt ikke anvise nogle supplerende tekniske foranstaltninger, der kan betragtes som effektive.

Derudover fastslår Datatilsynet i vejledningen, at det er nødvendigt for den dataansvarlige at være opmærksom på, om cloudleverandører beliggende indenfor EU/EØS kan blive mødt med anmodninger om adgang til personoplysninger fra et tredjeland. Det kan fx være på baggrund af cloudleverandørens koncernstruktur, hvor moderselskabet er etableret i et tredjeland. Dette vil for eksempel være tilfældet for amerikanske cloudleverandører i henhold til US Cloud Act. En sådan overdragelse til et tredjelands myndigheder vil efter Datatilsynets opfattelse være et brud på persondatasikkerheden.

NJORDS BEMÆRKNINGER

Selvom Datatilsynets nye vejledning om brugen af cloudservices kommer vidt omkring de udfordringer, der er forbundet med brugen heraf, må vi konstatere, at den ikke bibringer meget nyt. Brugere af cloudservices i tredjelande, herunder særligt USA, står fortsat over for de samme udfordringer i forhold til overførsel af personoplysninger udenfor EU/EØS, og vejledningen anviser ikke en reel løsning på dette.

NIS PETER DALL
ADVOKAT (L), PARTNER

(+45) 77 40 10 18
NPD@NJORDLAW.COM

PERNILLE KIRK ØSTERGAARD
ADVOKAT, SENIORSPECIALIST

(+45) 77 40 11 74
POS@NJORDLAW.COM