Personvern – Binding Corporate Rules:

Overføring av person-opplysninger til utlandet

Stadig flere norske selskaper overfører personopplysninger ut av Norge og ut av EU/ EØS. Er sikringen av opplysningene og personvernvernet viet den oppmerksomheten som dette krever?

Artikkelen er forfattet av:

Advokat
Bjørn Ofstad
Deloitte Advokatfirma

Personopplysningsloven definerer personopplysninger som opplysninger og vurderinger som kan knyttes til en enkeltperson, eksempelvis et selskaps registrerte opplysninger om egne ansatte eller kunder. Det er ikke lov å behandle andres personopplysninger med mindre det finnes et grunnlag for behandlingen. Et slikt grunnlag kan eksempelvis være samtykke fra den som får sine personopplysninger behandlet, eller hjemmel i lov.

Stadig flere norske selskaper overfører personopplysninger ut av Norge og ut av EU/EØS. Eksempelvis benyttes fjernsupportløsninger for IT-drift i India, eller vi ser eksempler på at internasjonale konsern har sentralisert personaladministrasjonen for alle deler av konsernet i lavkostland øst i Europa. Det kan være flere grunner til dette: jakten på kompetanse eller ønske om å kutte kostnader, er to eksempler. Et betimelig spørsmål er hvorvidt sikringen av opplysningene og personvernvernet er viet den oppmerksomhet som slik behandling krever. Overføring av personopplysninger til utlandet er å anse som en behandling av personopplysninger, med den konsekvens at personopplysningsloven får anvendelse. Så fremt personopplysningslovens generelle krav til behandling av personopplysninger er oppfylt, eksempelvis at virksomheten har et grunnlag til i det hele tatt å ha et elektronisk kunderegister, kan personopplysninger overføres til land som sikrer en forsvarlig behandling av opplysningene, jf. personopplysningslovens § 29 første ledd. Alle EU- og EØS-land anses for å ha en forsvarlig behandling, i kraft av å ha gjennomført personverndirektivet. Personopplysninger kan også overføres til land som Europakommisjonen har godkjent, eksempelvis Sveits, Canada og Argentina, og enkeltbedrifter i USA som er sertifisert etter Safe Harbor-prinsippene. Dette er prinsipper som legger opp til en selvsertifisering med mulig etterkontroll. At en virksomhet i USA erklærer å følge Safe Harbor-prinsippene fastsatt av amerikanske myndigheter anses av EU kommisjonen å sikre et tilstrekkelig vernenivå for personopplysninger.

Ved overføring av personopplysninger til land som ikke anses for å ha en forsvarlig behandling av personopplysninger, er lovens utgangpunkt at den som får sine opplysninger behandlet, må samtykke til overføringen. Ofte er dette ikke en særlig god løsning for den som ønsker å overføre opplysningene. Et annet mer relevant alternativ er at Datatilsynet kan tillate overføring dersom den behandlingsansvarlige gir tilstrekkelige garantier for vern av den registrertes rettigheter, jf. personopplysningslovens § 30 annet ledd. Dersom både den norske og den utenlandske virksomheten underskriver en avtale for overføring til utlandet og håndteringen av opplysningene som overføres, vil Datatilsynet legge til grunn at det er stilt tilstrekkelig garantier for den registrertes personvern, og overføringen vil tillates. Det finnes standardkontrakter til slikt bruk, og ved en slik fremgangsmåte er ansvaret for behandlingen av opplysningene plassert.

Binding Corporate Rules

Bruk av standardkontrakter vil i mange tilfeller være en hensiktsmessig måte å sikre en forsvarlig behandling av personopplysninger utenfor EU/EØS, eller de land som ikke er godkjent av EU. I de tilfellene det er tale om flere overføringer til flere land, vil den som skal holde oversikten over dataflyten lett miste oversikten ved bruk av ovennevnte metode. I slike tilfeller vil bruk av Binding Corporate Rules (BCR) være et godt instrument, som også av Datatilsynet anses å gi et tilstrekkelig vern av den registrertes rettigheter, jf. personopplysningslovens § 30 annet ledd.

BCR er konsern- eller selskapsinterne regler som regulerer håndtering av personopplysninger på en ensartet måte i hele den globale selskapsstrukturen. BCR skal gi et sett med personvernprinsipper og omtale av prosedyrer som skal trygge etterlevingen i praksis. Eksempelvis skal BCR regulere hvem som har ansvaret for personopplysningene, hvilke opplysninger som behandles i konsernet, hva opplysningene kan brukes til, hvilke land opplysningene kan overføres til og hvor lenge opplysningene kan lagres. BCR blir på en måte en utvidet internkontroll, noe alle virksomheter som behandler personopplysninger er forpliktet til å ha.

Før bindende konsernregler er klare for bruk, kreves godkjenning fra Datatilsynet, som igjen må ha en godkjenning fra minst én annen personvernmyndighet innen EU. BCR er anbefalt av Datatilsynet, men det er i dag kun noen få virksomheter som så langt har benyttet seg av ordningen. Forslag til endringer i lovverket indikerer imidlertid at det skal bli lettere å få BCR på plass, og er etter vår oppfatning en

OVERFØRER PERSONOPPLYSNINGER: Stadig flere norske selskaper overfører personopplysninger ut av Norge og ut av EU/EØS.

indikasjon på at man ønsker at flere virksomheter skal ta i bruk BCR.

Det ligger litt jobb bak å få BCR på plass, men når jobben først er gjort, står man overfor en tidløs ordning som tillater fri flyt av opplysninger på kryss og tvers i den globale organisasjonen. Ordningen er blant annet mye brukt i land som Tyskland, Frankrike og Storbritannia.

Ny personvernforordning

Forslag til ny personvernforordning er lagt frem i EU og vil ved ikrafttredelse også få konsekvenser i Norge. Blant forslagene i den nye forordningen ligger en forankring av dagens praksis av BCR i personvernlovgivningen.

I forslag til ny personvernforordning ligger også justering av Datatilsynets mulighet til å sanksjonere mot brudd på behandling av personopplysninger. Datatilsynet har i dag mulighet til å fatte vedtak om overtredelsesgebyr på inntil 10G (ca. 850 000 kr) for den som overtrer personopplysningsloven eller forskrift til loven. I forslag til ny personvernforordning foreslås det at det skal kunne gis overtredelsesgebyr på opp mot 5 % av global omsetning. Da begynner det å bli dyrt ikke å følge personopplysningslovens reguleringer av håndtering av personopplysninger.