Lov & Data

Nr. 150
September 2022

Nr. 3/2022

Innhold

Lov&Data

Lov&Data er et skandinavisk tidsskrift for rettsinformatikk og utgis av

Lovdata
Postboks 6688 St. Olavs plass
NO-0129 Oslo, Norge
Tlf.: +47 23 11 83 00
E-post: lovogdata@lovdata.no
Nettside: www.lovdata.no

Trykk: ISSN 0800-7853
Elektronisk: ISSN 1503-8289
Utkommer med 4 nummer pr. år.

Abonnementspriser for 2022
Norge: nkr 385,- pr. år
Utland: nkr 468,- pr. år
Studenter, Norge: nkr 182,- pr år
Studenter, utland: nkr 244,- pr. år
Alle fritt tilsendt.

Lov&Data sendes gratis til ordinære abonnenter av Lovdata Pro og er medlemsblad for foreningene Norsk forening for jus og edb, Svenska föreningen för IT och Juridik (ADBJ), Dansk forening for Persondataret og Danske IT-advokater.

Foreningene kan ev. sende låste pdf-er til sine medlemmer.

Abonnenter på papirutgaven av Lov&Data kan ved henvendelse til Lovdata/sin forening få passord som gir tilgang til elektroniske utgaver av tidsskriftet. Disse er tilgjengelige på *http://www.lovdata.no/pro/tidsskrift/*

Trykk og layout: 07 Media – 07.no

Leder

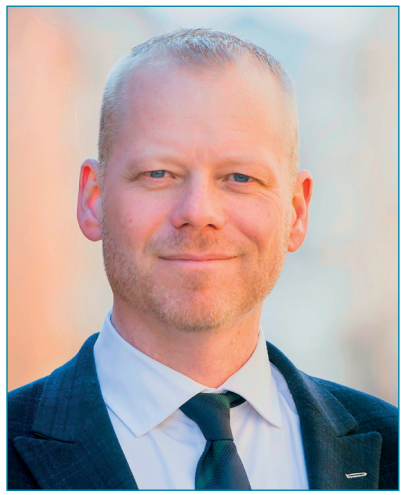
Dataskyddet som hinder mot maskininlärning och samhällsnyttig analys?

Många innovationer är idag kopplade till maskininlärning för att skapa artificiell intelligens (AI) och till andra kraftfulla analyser för att utvinna ny kunskap ur data. För att nå framgång krävs tillgång till stora datamängder som är relevanta och kompletta.

Politiskt finns det höga förväntningar på att en ökad användning av data ska kunna bidra till att lösa olika samhällsutmaningar. Både inom EU och på nationell nivå har det antagits strategier för att nyttiggöra data. På EU-nivå har strategin konkretiserat genom antagandet av ny lagstiftning och genom ytterligare förslag. Exempel på sådan lagstiftning är öppnadata-direktivet, Digital Governance Act och Data Act.

Dataskyddslagstiftningen är elefanten i rummet. Den vida definitionen av begreppet personuppgifter gör att lagstiftningen i många sammanhang blir tillämplig på såväl insamling och delning av data som användning för analys eller maskininlärning. Krav på uppgifts- och lagringsminimering och rättsligt stöd för behandling av varje uppgift verkar i många fall begränsande och skapar i andra fall åtminstone stor osäkerhet kring vilka projekt som är möjliga att genomföra.

Den nya lagstiftningen som syftar till att nyttiggöra data innehåller inga



Daniel Westman

undantag eller lättnadsregler för behandlingen av personuppgifter. Tvärtom tydliggörs att dataskyddslagstiftningen är fullt tillämplig.

Det råder ingen tvekan om att det finns risker förknippade med att samla stora mängder personuppgifter, men samtidigt är det viktigt att påpeka att enskilda individers egenskaper eller agerande inte står i fokus vid dessa former av analys. Uppgifterna används som en resurs för att utvinna kunskap på en högre nivå. Utförs hanteringen på rätt sätt har användningen heller ingen negativ effekt på de berörda personerna. Vi har alltså här att göra med en annan typ av behandling än den som t.ex. är inriktad mot att samla stora mäng-

der uppgifter om individer i syfte att erbjuda annonsörer att rikta marknadsföring. Precis som när det gäller t.ex. statistik och många typer av forskning innehåller slutprodukten – om arbetet utförs på rätt sätt – inte några personuppgifter.

Möjligheten att leva upp till den gällande dataskyddsregleringen varierar naturligtvis från projekt till projekt.

Framför allt är det finalitetsprincipen (kravet på ändamålskoppling), kravet på rättsligt stöd för behandlingen av "vanliga" personuppgifter och kravet på särskilt rättsligt stöd för behandling av känsliga personuppgifter som skapar direkta hinder eller stor osäkerhet. I praktiken är det sällan en framkomlig väg att basera de aktuella behandlingarna på samtycke. Det beror bl.a. på att många enskilda berörs och att möjligheterna att få ett giltigt samtycke från tillräckligt många för att säkerställa ett representativt urval i praktiken är begränsade. Samtidigt är det ofta osäkert om andra mer lämpliga rättsliga grunder, t.ex. uppgift av allmänt intresse eller legitimt intresse (intresseavvägningen), omfattar den delning och analys som ska göras.

I vissa fall är det möjligt att anonymisera personuppgifter innan de används för maskininlärning eller analys. Många gånger är det emellertid svårt för den personuppgiftsansvarige att bedöma om ett försök till anonymisering har lyckats. EU-domstolens vida tolkning av begreppet personuppgifter (Breyer-målet) i kombination med en utveckling där det finns allt fler tillgängliga datamängder som någon kan använda för återidentifiering gör läget komplicerat.

Det finns vissa tillvägagångssätt för att minska behovet av att använda och att dela personuppgifter på ett sätt som är problematiskt enligt dataskyddslagstiftningen. Ett är att använda syntetiska data, dvs. data som har samma karaktär som riktiga uppgifter men som inte avser verkliga människor. Ett annat är att använda federerad maskininlärning, vilken innebär att data inte behöver överföras mellan organisationer och samlas i en enda stor databas. Enkelt uttryckt flyttas istället själva maskininlärningsverksamheten runt. Men inget av dessa tillvägagångssätt utgör någon patentlösning för att hantera alla dataskyddsrättsliga utmaningar.

Viss osäkerhet och obefogad restriktivitet kan hanteras genom praxis och vägledning från dataskyddsmyndigheterna. Integritetsskyddsmyndigheten arbetar t.ex. med ett intressant uppdrag om kunskapshöjande insatser för innovationsprojekt.

Min bedömning är dock att det också krävs rättsliga reformer för att dataskyddslagstiftningen inte ska fungera som ett omotiverat hinder mot effektiv maskininlärning och kraftfull analys av stora datamängder. Exakt vad som bör göras måste naturligtvis utredas närmare – inte minst för att hitta rätt balans mellan innovation och skydd för enskilda individer – men låt mig skissa på två möjliga åtgärder.

- Gör hantering av data tillåten om den personuppgiftsansvarige vidtagit vissa anonymiseringsåtgärder som räknas upp t.ex. i en s.k. delegerad akt från EU-kommissionen. Vilka åtgärder som listas måste bestämmas utifrån tillgänglig teknik för återidentifiering vid varje given tidpunkt. Data som varit föremål för den aktuella typen av anonymiseringsåtgärder ska även få delas till en annan aktör som utför maskininlärningen eller analysen. Fördelen med den föreslagna ordning är en större förutsebarhet för den personuppgiftsansvarige samtidigt som utvecklingen och användningen av anonymiseringstekniker främjas, vilket även gagnar alla berörda individer.
- Inför kompletterande EU-reglering som tydliggör att maskininlärning och kraftfull analys av stora mängder personuppgifter får ske för samhällsnyttiga ändamål. Ett villkor bör vara att behandlingen syftar till att utvinna aggregerad kunskap på gruppnivå och att slutresultatet av behandlingen inte innehåller några personuppgifter. Förutsättningarna liknar på många sätt de som gäller behandlingen av personuppgifter för statistiska ändamål. Säkerhets- och skyddsåtgärder för att motverka de risker som finns kan t.ex. vara pseudonymisering, korta gallringstider, förbjud mot att använda insamlande personuppgifter för att vidta åtgärder rörande de registrerade och särskilda krav på åtkomstbegränsning.

Det finns säkert invändningar och konstruktiva motförslag. Det är bra eftersom vi behöver en diskussion om hur vi kan hitta rätt balans mellan datadriven innovation och skyddet för personuppgifter.

Daniel Westman

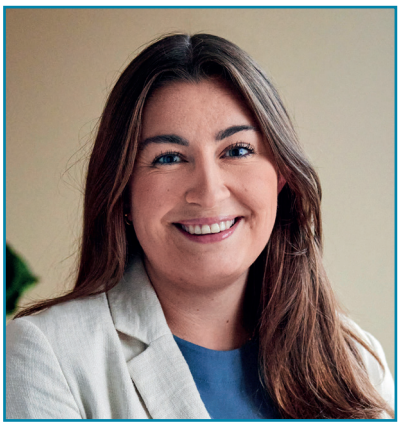
Åpen og rettferdig Kunstig intelligens

Av Thale Cecilia Gautier Gjerdsbakk

Denne artikkelen er den første i en serie på tre artikler om kunstig intelligens og hvordan det utfordrer rettferdighets- og åpenhetsprinsippet i personvernforordningen art. 5 nr. 1 (a).1 De neste artiklene vil bli publisert i Lov&Datas 4. utgave 2022 og 1. utgave 2023.

Dagens teknologi gjør det mulig å samle inn, dele og sammenstille store mengder personopplysninger og andre data.[2] Denne muligheten har gitt grobunn for utviklingen av kunstig intelligens (KI) på et nytt nivå. KI har et vidt anvendelsesområde; det kan bidra til alt fra å effektivisere byråkratiske prosesser til å hjelpe leger med å forutsi faren for hjertesvikt. KI har åpenbare fordeler, og brukes stadig mer.[3] For eksempel blir KI stadig oftere benyttet til beslutningsstøtte, nettopp av effektiviseringshensyn. Denne artikkelserien tar derfor for seg KI brukt som beslutningsstøtte.

Bruken av KI innebærer imidlertid utfordringer for personvernet.



Thale Cecilia Gautier Gjerdsbakk

Manglende transparens og urettferdighet trekkes gjennomgående frem som problematiske forhold ved KI. Artikkelserien skal derfor sette søkelys på manglende transparens og urettferdighet ved bruk av KI som beslutningsstøtte. I første omgang vil jeg trekke frem noen elementer ved utviklingsmetoden av KI som gjør det utfordrende å overholde åpenhets- og rettferdighetsprinsippet.[4]

1. Retten til åpen og rettferdig behandling av personopplysninger

Prinsippene om åpenhet og rettferdighet fremgår av det som gjerne kalles for personvernets grunnlov: personvernforordningens grunnleggende prinsipper i art. 5. Prinsippene legger premissene for hva som er lovlig behandling av personopplysninger.

Kravet om åpenhet er viktig for at den registrerte skal forstå hva som skjer med sine opplysninger. Åpenhetskravet er todelt. For det første forutsetter åpenhet at behandlingsansvarlig gir informasjon om behandlingen av personopplysninger (innholdskrav).[5] For det andre må informasjonen være forståelig for den registrerte (formkrav).[6] Åpenhet er essensielt for å skape tillit til behandlingsprosessen og er en forutsetning for at den registrerte kan vurdere om behandlingen tilfredsstiller personvernforordningens krav.

Ordet «rettferdig» i personvernforordningen art. 5 (1) a) tilsier at behandlingen må være rimelig og ligge innenfor de moralske og etiske normene som følger av lover og regler, men også innenfor samfunnets rettferdighetsoppfatning. Utover dette er rettferdighet et vidt begrep med et bredt anvendelsesområde. Rettferdighet innebærer blant annet krav til lovlighet, åpenhet, fravær av uønsket forskjellsbehandling og at det tas hensyn til asymmetrisk maktbalanse. Videre spiller etikk og moral, kultur og kontekst inn på hva som oppfattes som rettferdig.

> Åpenhet er essensielt for å skape tillit til behandlingsprosessen og er en forutsetning for at den registrerte kan vurdere om behandlingen tilfredsstiller personvernforordningens krav.

Ettersom personvernforordningen er teknologinøytral, omfatter kravene i forordningen også be-

1 Europaparlamentets og Rådets forordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF [personvernforordningen].

2 Personvernforordnongens fortalepunkt 6.

3 NOU 2020:11 Den tredje statsmakt – Domstolene i endring, s. 254.

4 Personvernforordningen art. 5 nr. 1 (a).

5 Personvernforordningen art. 13 og 14.

6 Personvernforordningen art. 12 nr. 1.

handling av personopplysninger ved hjelp av ny teknologi, som KI. Bruk av KI som beslutningsstøtte må altså tilfredsstille både form- og innholdskravet for åpenhet, samt alle aspektene ved rettferdighetskravet.

2. Hvordan utvikles KI?

For å forstå åpenhets- og rettferdighetsutfordringene KI medfører er det nødvendig med en minimumsforståelse av hvordan KI utvikles.

De siste årene har *maskinlæring* og dyplæring (samlet omtalt som maskinlæring) blitt de vanligste måtene å utvikle KI på. Maskinlæring skaper utfordringer for åpenhet- og rettferdighet blant annet fordi programvaren lærer fra erfaringer og kan handle uten å bli spesifikt programmert.[7] Når man utvikler maskinlæringssystemer gir man et system av algoritmer tilgang på data (input) som systemet på egenhånd analyserer og trekker ut erfaringer fra, basert på mønstre og sammenhenger i dataene.[8] Algoritmene lærer fra dataene, og forbedrer seg selv ved at parameterne i algoritmene justeres ettersom den ser flere læringseksempler. Gjennom prøving og feiling blir systemet mer og mer nøyaktig.[9]

Denne prosessen kalles å trene algoritmen. Når en algoritme er tilstrekkelig trent, klarer den å prosessere ukjent informasjon og komme med et eget, og forhåpentligvis korrekt svar (output).

Historiske data brukes ofte til treningen, ettersom maskinlæring krever store mengder treningsdata. For eksempel kan programmererne gi algoritmene tilgang på de faktiske hendelsene og resultatet i alle fengslingskjennelser fra 1900 og frem til i dag. Algoritmene vil da analysere de faktiske hendelsene og se hvilke faktorer som går igjen for de utfallene der gjerningspersonen blir dømt. Dommene fra 1900-1950 kan for eksempel vise at det var større sannsynlighet for å bli dømt om man ikke brukte briller. Dommene fra 1950-2000 kan eksempelvis vise at dersom den fornærmede var ektefellen til gjerningspersonen, var det større sannsynlighet for domfellelse. I tillegg kan det vise det seg at de ektefellene som var arbeidsledige oftere ble dømt enn de som hadde en jobb. Algoritmene vil da tolke dette som at brillebruk tilsier at man ikke skal dømmes, mens en ektefellerelasjon til fornærmede og arbeidsledighet vil tale for å dømme den tiltalte.

> Algoritmene lærer fra dataene, og forbedrer seg selv ved at parameterne i algoritmene justeres ettersom den ser flere læringseksempler. Gjennom prøving og feiling blir systemet mer og mer nøyaktig.

Det er flere faktorer som kan påvirke hvor treffsikker KI-en blir. Resultatene kan bli mer treffsikre jo mer data algoritmene lærer fra.[10] Treffsikkerheten avhenger også av dataenes kvalitet og hvordan dataene er bygget opp.[11] Dersom det bare hadde vært mengden data som avgjorde hvor treffsikker algoritmene blir, kunne man tenkt seg at det var nyttig å trene KI-en på kinesiske fengslingskjennelser, som det jo finnes mange av. Men fordi kinesisk domspraksis og lover avviker fra våre, vil de kinesiske dataene neppe egne seg til å si noe om den norske befolkningen eller norsk domspraksis. Dersom de kinesiske kjennelsene viser at myndighetskritikere oftere fengsles, lærer algoritmen seg at det er riktig løsning. Dermed ville ikke en algoritme trent på kinesiske data oppfylt de norske kravene til rettferdighet. Store mengder data er en forutsetning for å trene algoritmen, men en godt trent algoritme vil være verdiløs om dataene den trenes på har for dårlig kvalitet eller ikke tilpasses.

Når algoritmer trenes dannes det nevralaktige nettverk. Nettverkene består av ulike inputfaktorer og sammenhengen mellom disse.[12] Fra eksempelet over kan det være sammenhengen mellom at gjerningspersonen er ektefellen til fornærmede og at vedkommende ikke bruker briller. De nevrale nettverkene er bygget opp med ett inputlag (de faktiske hendelsene i eksempelet over), flere skjulte lag (sammenhengen mellom brillebruk og relasjon til fornærmede) og ett outputlag (domsresultatet). Algoritmene er i stand til å se sammenhenger som mennesker ikke klarer å fange opp på grunn av de store datamengdene systemet klarer å prosessere.[13]

Mens en dommer kanskje merker seg at ektefeller ofte blir fengslet, er det ikke sikkert de ser sammenhengen mellom at de som bruker briller fengsles sjeldnere. Jo mer data KI-en får trene algoritmene på, jo flere lag med nettverk kan dannes, og jo flere lag med nettverk som dannes, jo «dypere» blir nettverkene.[14]

7 Bendiksen, Christian & Hansen, Eirik Norman, *Når juss møter AI*, Gydendal 2019, s. 19.

8 Datatilsynet *Kunstig intelligens og personvern*, publisert januar 2018. Tilgjengelig på: *https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/rettigheter-og-plikter/rapporter/rapport-om-ki-og-personvern.pdf* (lest 26.08.2022), s. 6.

9 NOU 2020:11 s. 254.

10 Datatilsynet (2018), s. 10.

11 Ibid.

12 Bendiksen og Hansen (2019), s. 19.

13 NOU 2020:11, s. 254.

14 Datatilsynet (2018), s. 13.

3. Den sorte boksen og algoritmeskjevhet

Algoritmene justerer selv vekten mellom parameterne i lagene.[15] Når nettverkene blir dype nok, blir modellen så komplekst sammensatt at mennesker ikke klarer å forstå hvilke sammenhenger og tilpasninger algoritmen gjør i de ulike lagene.[16] Det ville tatt mennesker uoverkommelig lang tid å regne ut matematikken bak et stort nevralt nettverk. Dette gjør det umulig selv for utviklerne av KI-en å forklare hvorfor systemet løste oppgaven som den gjorde.[17] Det er kompleksiteten av modellen, som blant annet kommer av de dype nevrale nettverkene, som danner grunnlaget for «den svarte boks' problem».[18] Vektingen og justeringen algoritmen gjør i de skjulte lagene medfører at beslutningsprosessen til KI-en er like ugjennomsiktig som en svart boks. Dette gjør det utfordrende å oppfylle personvernforordningens krav til åpenhet.

> Algoritmene er i stand til å se sammenhenger som mennesker ikke klarer å fange opp på grunn av de store datamengdene systemet klarer å prosessere.

15 Ibid., s. 11.
16 NOU 2020:11 s. 254
17 Datatilsynet (2018), s. 12.
18 Ibid.

Det er ikke bare hvordan de ulike faktorene vektes mot hverandre som kan medføre at algoritmene gir uønskede svar, men også *hvilke* faktorer som tillegges vekt. Et eksempel er en algoritme som ble trent til å klassifisere bilder av hunder og ulver. Resultatet av KI-ens analyse var at bildene med snø i bakgrunnen oftest ble klassifisert som ulvebilder.[19] KI-en vektla altså en irrelevant faktor for å bestemme utfallet. I eksempelet over reagerte du sikkert på at det var større sannsynlighet for å bli fengslet dersom du ikke bruker briller. Hvor godt eller dårlig syn du har skal jo ikke ha noe å si for om du oppfyller straffeprosesslovens vilkår for fengsling. Ettersom det i praksis ikke er mulig å forklare hvordan KI-en har løst oppgaven den har fått, vet vi heller ikke hvilke faktorer KI-en har vektlagt for å avgjøre spørsmålet.

Selv om KI tar beslutninger langt raskere, og tar hensyn til langt flere faktorer og sammenhenger enn det mennesker klarer, er den ikke feilfri.[20] Feilene stammer gjerne fra at dataene som brukes for å trene KI-en ikke er gode nok, eksempelvis at dataen er mangelfull eller inneholder skjevheter eller diskriminering.[21] KI-en vil da lære av den diskriminerende praksisen, og kan skape eller forsterke uønsket forskjellsbehandling. Algoritmeskjevhet (på engelsk «machine bias») kan defineres som systematiske og gjentatte feilslutninger i KI-systemer som medfører uønskede utfall, eksempelvis at en gruppe mennesker prioriteres over en annen.

Dette utfordrer retten til rettferdig behandling av personopplysninger.

> Algoritmeskjevhet (på engelsk «machine bias») kan defineres som systematiske og gjentatte feilslutninger i KI-systemer som medfører uønskede utfall, eksempelvis at en gruppe mennesker prioriteres over en annen.

19 Ribeiro, Singh og Guestrin, «*Why Should I Trust You?» Explaining the Predictions of Any Classifier*, publisert august 2016. Tilgjengelig på: *https://arxiv.org/pdf/1602.04938.pdf* (lest 26.08.2022), punkt 6.4.
20 NOU 2020:11, s. 254.
21 Ibid.

4. Oppsummering

Du vet nå at utvikling av KI krever mye data av høy kvalitet, og at måten KI lærer på i praksis ofte gjør det umulig å forklare logikken bak algoritmens slutninger. Du ser derfor også antagelig hvordan KI gir noen utfordringer når åpenhets- og rettferdighetsprinsippet skal oppfylles. Neste artikkel vil gå dypere inn i åpenhetsprinsippet og de utfordringene som oppstår i møtet mellom KI og åpenhet.

Thale Cecilia Gautier Gjerdsbakk er advokatfullmektig med spesialisering innen personvern, teknologi og KI i advokatfirmaet BULL. tcgg@bull.no

Nytt om digital tillgänglighet

Av Johanna Wallin

1 Inledning

Tidigare i år publicerades proposition 2021/22:119 *Modernare regler för användningen av tvångsmedel* till regeringens förslag på lagändringar avseende tvångsmedel som lades fram i december förra året.[1] Förslaget kom som en reaktion på att teknikutvecklingen bidragit till att brottsligheten blivit alltmer svår och komplex att utreda och lagföra.

En angränsande fråga behandlades i Mål Ö 4651–21 ”Årsopgørelserna” där Högsta domstolen (HD) biföll ett yrkande om edition avseende elektroniskt lagrade handlingar i en utländsk myndighets molntjänst. HD gjorde bedömningen att svaranden fick anses inneha handlingarna.

2 HD:s dom

I målet, som rörde underhållsbidrag till barn, yrkade käranden att tingsrätten skulle förelägga svaranden att inkomma med elektroniska handlingar från den danska skattemyndigheten. Svaranden bestred i sin tur editionsyrkandet och invände att han inte hade handlingarna och vidare saknade möjlighet att få tillgång till dessa, och att han därför inte kunde betraktas som innehavare av handlingarna. Editionsyrkandet ogillades av tingsrätten och dom meddelades, vilken sedermera, efter överklagande till hovrätten, kom att ändras vad gäller editionsfrågan. Svaranden överklagade senare hovrättens dom till HD som meddelande prövningstillstånd.[2]

Johanna Wallin

HD prövade bl.a. frågan om vad som krävs för att en person ska anses inneha en elektronisk handling på ett sådant sätt som utgör en förutsättning för edition, och gick inledningsvis igenom allmänna förutsättningar för edition[3], och dess tillämplighet på elektroniskt lagrade handlingar[4], samt domstolars rätt att utfärda förelägganden.[5]

HD övergick därefter till att närmare redogöra för förutsättningarna i frågan om innehavskravet. HD konstaterade att endast den som innehar en handling kan föreläggas att förete den, men att ägandet av handlingen inte utgör någon förutsättning för innehav. I stället räcker det att personen *”på ett fysiskt eller jämförbart sätt har tillgång till handlingen genom att i allmän mening ha handlingen i sin besittning”* för att innehavskravet ska anses uppfyllt.

> Uppdateringen innebär bl.a. att förbudet mot att beslagta meddelanden mellan den misstänkte och en närstående avskaffas, en ny skyldighet för enskilda att under vissa förutsättningar medverka till biometrisk autentisering, en möjlighet att förelägga enskilda att tillhandahålla handlingar under ett tidigare stadium i en förundersökning samt en ny möjlighet att under vissa förutsättningar dröja med underrättelse om att tvångsmedel använts.

HD konstaterade vidare att det för handlingar som finns lagrade i elektronisk form, t.ex. i en molntjänst eller extern databas, räcker att editionssvaranden har en *”på lag eller avtal grundad ovillkorlig rätt till handlingen och kan få tillgång till information t.ex. genom inloggning”* för att innehavskravet ska vara uppfyllt.[6]

HD konstaterade även i sin redogörelse förinnehavskravet att den digitala utvecklingen har inneburit

1 Lagrådsremiss Modernare regler för användningen av tvångsmedel, publicerad den 1 december 2021.

2 Högsta domstolens dom Mål nr Ö 4651–21, meddelat i Stockholm den 8 april 2022, p. 1–3.

3 Huvudregeln är att den som innehar en skriftlig handling, som kan antas ha betydelse som bevis, är skyldig att förete den (38 kap. 2 § rättegångsbalken).

4 Förhållandet att uppgifter är elektroniskt lagrade utgör inte ett hinder för att utskrifter avseende uppgifterna görs till föremål för edition, jfr. NJA 1998 s. 829 ”Loggfilerna”.

5 Mål nr Ö 4651–21, p. 5–10.

6 Mål nr Ö 4651–21, p. 11–13.

att förvaring av fysiska handlingar hos en person alltmer ersatts av förvaring hos tredje man – i elektronisk form. Handlingar lagras eller hanteras idag ofta genom IT-tjänster, t.ex. molntjänster.

3 Modernare regler för användning av tvångsmedel

Det är intressant att HD:s dom och klargörandet kring innehavskravet kom i samband med publiceringen av propositionen om modernare regler för användningen av tvångsmedel.

Syftet med ändringarna är att uppdatera och modernisera regleringen av användning av tvångsmedel. Uppdateringen innebär bl.a. att förbudet mot att beslagta meddelanden mellan den misstänkte och en närstående avskaffas, en ny skyldighet för enskilda att under vissa förutsättningar medverka till biometrisk autentisering, en möjlighet att förelägga enskilda att tillhandahålla handlingar under ett tidigare stadium i en förundersökning samt en ny möjlighet att under vissa förutsättningar dröja med underrättelse om att tvångsmedel använts. Mest intressant är kanske införandet av ett nytt tvångsmedel: *genomsökning på distans* – vilket kan säkra tillgång till elektroniska handlingar i t.ex. molntjänster eller externa servrar.

Det nya tvångsmedlet *genomsökning på distans* tänkt att införas och definieras i 28 kap. rättegångsbalken (1942:740) som sökning efter handlingar som *”finns lagrade i ett avläsningsbart informationssystem utanför den elektroniska kommunikationsutrustning som används för att utföra genomsökningen”*. Under förutsättning att det finns anledning att anta att ett brott har begåtts på vilket fängelsestraff kan följa får genomsökning på distans genomföras, ett sådant beslut fattas av undersökningsledare, åklagare eller av rätten. Genomsökningen ska utföras i ett avläsningsbart informationssystem som den som skäligen misstänks kan antas ha använt (10 a-10 d §§).[7]

Biträdande jurist Johanna Wallin, Wikström & Partners Advokatbyrå.

7 Proposition 2021/22:119, Modernare regler för användningen av tvångsmedel, s. 14 f.

Unntak fra rett til informasjon og innsyn i personopplysninger av hensyn til etterforskning mv. av straffbare handlinger

Av Ove A. Vanebo

1. Innledning

EUs personvernforordning (EU) 2016/679 (heretter bare «forordningen») er gjennomført i norsk rett gjennom personopplysningsloven § 1. Forordningen gir registrerte personer rett til blant annet å bli informert når personopplysninger om dem samles inn og få innsyn i personopplysningene og informasjon om bruken av dem, jf. artiklene 13, 14 og 15. Etter personopplysningsloven er det imidlertid en rekke unntak fra rett til å motta informasjon og kunne få innsyn.

Et prinsipielt viktig unntak fra retten til informasjon og innsyn, er at «det er påkrevd å hemmeligholde [opplysninger] av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger», jf. personopplysningsloven § 16 første ledd bokstav b. Unntaket favner vidt, og knytter seg ikke til nærmere behandlingsformål, kategorier av behandling, kategorier av personopplysninger eller lagringsperioder.[1]

Reguleringen er i hovedsak en videreføring av personopplysningsloven 2000 § 23 første ledd bokstav b.[2] Unntaket er utformet innenfor rammene av adgangen til å gi unntak etter artikkel 23 nr. 1 bokstav d, som gjelder «forebygging, etterforskning, avsløring eller straffeforfølgning av straffbare forhold».

Ove A. Vanebo

Bestemmelsen er utvilsomt viktig, siden informasjons- og innsynsrett i noen tilfeller kan spolere avdekking og forfølging av straffbare handlinger, f.eks. hvis mistenkte personer får innsyn i at de overvåkes eller at sak forberedes mot dem.

Under vil jeg gi en redegjørelse for unntakets innhold og rekkevidde.

2. Hvilke handlinger kan gi grunnlag for å benytte unntaket?

Unntaket vil kunne begrunne hemmelighold av opplysninger ved nær sagt enhver handling som skjer for å avdekke eller forfølge straffbare forhold. Personvernrådet synes å uttrykke at forordningen tillater å lage unntak for en rekke ulike aktiviteter, og nevner at art. 23 nr. bokstav d «is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories».

«Forebygging» vil trolig omfatte de fleste preventive tiltak for å redusere kriminalitet, f.eks. ulike former for logging eller registrering av mistenkelig aktivitet.

> Et prinsipielt viktig unntak fra retten til informasjon og innsyn, er at «det er påkrevd å hemmeligholde [opplysninger] av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger»

I Norge har «etterforskning» tradisjonelt blitt tolket snevert, til etterforskning i straffeprosesslovens forstand.[3] I EU-domstolens dom av 7. november 2013 (C-473/12, *Institut professionel des agents immobiliers*), synes imidlertid retten å gå langt i å mene at man skal forstå aktivitetene vidt. Retten vurderte om det tilsvarende unntaket i personverndirektivet omfattet en privatdetektiv som opptrer for et profesjonsorgan for å etterforske og avsløre brudd på etiske regler for et lovregulert yrke. EU-domstolen kom til at organet og privatdetek-

1 Se Prop. 56 LS (2017–2018) s. 62, jf. forordningen artikkel 23 nr. 2 bokstav a, b og f.

2 Prop. 56 LS (2017–2018) s. 62.

3 Ot.prp.nr.92 (1998–1999) s. 121.

tivene som opptrer på vegne av organet, ikke vil være underlagt plikten til å gi informasjon til den registrerte personen, gitt at en stat har implementert et slik unntak ved forebygging, avsløring mv. Jeg antar at denne forståelsen også vil gjelde «etterforskning» og «avsløring» etter dagens personopplysningslov, særlig siden det nå er klart at private behandlingsansvarlige er omfattet av unntaket, se punkt 3 under.

Videre kan nevnes Personvernnemndas sak PVN-2021-02, der person ba om innsyn hos Justis- og beredskapsdepartementet. Departementet behandlet personopplysninger om en mann og hans familie i forbindelse med en internasjonal etterlysningssak og en utleveringssak fra utlandet til Norge. Departementet avviste innsyn blant annet fordi det var det nødvendig å unnta de aktuelle personopplysningene av hensyn til at den pågående straffesaken. Nemnda aksepterte at unntaket kunne forankres i personopplysningsloven § 16 første ledd bokstav b, og viste til at den manglet forutsetninger for å foreta en annen vurdering av unntaket for innsynsrett enn fagmyndigheten i dette konkrete tilfellet.

«Avsløring» av straffbare forhold vil sannsynligvis også favne bredt. Aktuelle aktiviteter er f.eks. sammenkobling av informasjon og deling av data mellom behandlingsansvarlige for å identifisere avvik.

3. Hvilke behandlingsansvarlige kan benytte unntaket?

I utgangspunktet åpner ordlyden i bestemmelsen for at enhver behandlingsansvarlig kan unnta informasjon og avstå fra å gi innsyn begrunnet avdekking av straffbare handlinger mv. I juridisk teori som gjelder personopplysningsloven av 2000 har det imidlertid vært antatt at private aktører, som f.eks. et forsikringsselskap, ikke kan benytte unntaket.[4] Johansen m.fl. viser til at personverndirektivet synes å knytte unntaksadgang til straffesaker, og at uttalelsene i forarbeidene tilsier at kun politi og kontrolletater kan benytte det.[5] I Ot.prp. 92 (1998-1999) s. 121 påpekte departementet at:

> Også Datatilsynet legger til grunn at private aktører kan benytte unntaket, og nevner som eksempel at en arbeidsgiver kan ha behov for å vente med å gi informasjon til registrerte i forbindelse med påståtte straffbare forhold, for eksempel økonomisk kriminalitet.

«Første ledd bokstav b gjør unntak for opplysninger som det er påkrevet å hemmeligholde av hensyn til å forebygge, etterforske, avsløre eller rettslig forfølge straffbare handlinger. Med etterforskning menes slik etterforskning som reguleres av straffeprosessloven kapittel 18. Bestemmelsen åpner også for unntak for å avdekke straffbare forhold som ledd i andre kontrolletaters virksomhet, jf f.eks toll- og ligningsvesenet.»

I forarbeidene til dagens personopplysningslov ble det imidlertid presisert at unntakets anvendelsesområde ikke «begrenses til nærmere bestemte kategorier av behandlingsansvarlige».[6]

Forordningen artikkel 23 nr. 1 bokstav d, som dagens bestemmelse er utformet innenfor rammene av, er heller ikke begrenset til noen bestemte kategorier av behandlingsansvarlige.

Også Datatilsynet legger til grunn at private aktører kan benytte unntaket, og nevner som eksempel at en arbeidsgiver kan ha behov for å vente med å gi informasjon til registrerte i forbindelse med påståtte straffbare forhold, for eksempel økonomisk kriminalitet. I et slikt tilfelle kan det være tillatt å vente med å gi informasjon til saken er meldt til politiet og etterforsket.[7]

4. Hva omfattes av «straffbare handlinger»?

Uttrykket «straffbare handlinger» vil trolig samsvare med handlinger (eller unnlatelser) som kan medføre sanksjon som er klassifisert som straff etter nasjonal lov.

I utgangspunktet er det avgjørende om lovgivningen betegner en rettsfølge som straff, jf. bl.a. straffeloven §§ 29 og 30 og militær straffelov § 12. Selv om en reaksjon ikke er straff i henhold til straffeloven mv., kan den likevel bli ansett som «straff» etter Grunnloven § 96. Jeg antar at det er tilstrekkelig at handlingen kan sanksjoneres med «straff» i Grunnlovens forstand. Den tradisjonelle oppfatningen er at lovgivers karakteristikk av en sanksjon normalt er avgjørende også i forholdet til Grunnloven.[8] Pønalt formål bak en sanksjon er ikke til-

4 Line Coll, i samarbeid med Dag Wiese Schartum, *Rettslige spørsmål knyttet til innsamling og bruk av digitale bevis*, 2004, s. 22-23. Se også Kommunal- og moderniseringsdepartementet, *Informasjonsplikt og innsynsrett etter personopplysningsloven; Veileder for offentlig sektor*, 2015, s. 23: «I slike tilfeller følger innsynsretten og informasjonsplikten reglene i straffeprosessloven.»

5 Michal Wiik Johansen, Knut-Brede Kaspersen og Åste Marie Bergseng Skullerud, *Personopplysningsloven; Kommentarutgave*, 2001, s. 177.

6 Prop. 56 LS (2017–2018) s. 62.

7 Datatilsynet, *Unntak frå retten til informasjon og innsyn*. Lest 30. august 2022: *https://www.datatilsynet.no/personvern-pa-ulike-omrader/personvern-pa-arbeidsplassen/intern-varsling/unntak-fra-retten-til-informasjon-og-innsyn/*

8 NOU 2003: 15 side 54 flg.

strekkelig til å klassifisere den som straff etter Grunnloven § 96, jf. Rt. 2014 s. 620 avsnitt 53.

Et særskilt spørsmål er imidlertid om handlinger som kan medføre administrative sanksjoner (eksempelvis overtredelsesgebyrer) som ikke anses som straff i henhold til straffelovene eller Grl. § 96, også kan være omfattet av «straffbare handlinger». Slike sanksjoner kan være «straff» i henhold til praksis fra Den europeiske menneskerettighetsdomstolen.[9] Den europeiske menneskerettskonvensjon med protokoller «skal gjelde som norsk lov», jf. menneskerettsloven § 2 nr. 1.

Personopplysningslovens formuleringer gir ingen klare svar. Problemstillingen er heller ikke omtalt i praksis, forarbeider eller teori, men bestemmelsens historikk og uttalelser tyder på at lovgiver så for seg at den internrettslige klassifiseringen i lov skulle være førende, jf. forarbeidenes uttalelser om unntak ved etterforskning etter straffeprosessloven.[10]

Svaret er imidlertid ikke åpenbart, og artikkel 23 nr. 1 bokstav d (som unntaket er utformet innenfor) åpner for å gjøre unntak i forbindelse med å avdekke og forfølge «criminal offences». Sistnevnte uttrykk vil fange opp også handlinger som medfører administrative sanksjoner, men som ikke formelt er kategorisert som «straff» i et lands nasjonale klassifikasjoner.[11]

5. Hva menes med at unntak må være «påkrevd»?

Den behandlingsansvarlige kan bare gjøre unntak i den utstrekning det er «påkrevd» i det enkelte tilfellet. Departementet mener kriteriet sørger for at unntaket er i tråd med kravene til nødvendighet og forholdsmessighet i forordningen artikkel 23 nr. 1.[12]

Datatilsynet har i sin praksis påpekt at «uttrykket "påkrevd" er et skjerpet nødvendighetsvilkår, som tilsier at unntaket skal anvendes med *stor forsiktighet*».[13] Tilsynet har derfor lagt til grunn at «påkrevd» er et «meget strengt vilkår», som «normalt innebærer en skjerpelse sam-

9 I henhold til Den europeiske menneskerettsdomstols avgjørelse Engel mfl. mot Nederland og etterfølgende praksis, skal det tas utgangspunkt i tre kriterier som skal vektlegges i vurderingen av om en sanksjon anses som «straff»: Klassifikasjonen etter nasjonal rett, den overtrådte handlingsnorms karakter, og innholdet og alvorligheten av reaksjonen. Se også Prop. 62 L (2015– 2016) s. 28.

10 Ot.prp.nr.92 (1998–1999) s. 121. Jeg hadde også en samtale med Datatilsynets veiledningstjeneste, som pekte på dette forhold, selv om en slik kort rådslagning ikke er avgjørende for tilsynets standpunkt om problemstillingen kommer på spissen.

11 EU-domstolens avgjørelse i sak C-439/19.

12 Prop. 56 LS (2017–2018) s. 62.

13 Endelig kontrollrapport fra Datatilsynet som gjelder NAV-direktoratet, saksnr. 12/00116, rapportdato 22. august 2012.

menlignet med uttrykket "nødvendig".[14] Det må trolig foreligge konkrete holdepunkter for at oppnåelse av formålet ellers blir vanskelig- eller umuliggjort. Antageligvis vil det her være relevant å se hen til hvor stor skaden eventuelt vil bli ved å gi innsyn.[15] Litt enkelt sagt, vil dette innebære også at ulike former for oppfølging for å håndtere straffbare handlinger, ikke kan legitimere hemmelighold dersom det ikke er grunn til å frykte bevisforspillelse, vitnetilpasning osv.[16]

> Tilsynet har derfor lagt til grunn at «påkrevd» er et «meget strengt vilkår», som «normalt innebærer en skjerpelse sammenlignet med uttrykket "nødvendig"»

Et særskilt spørsmål er om bruken av unntaket kan differensieres på bakgrunn av hvem som skal ha informasjon eller begjærer innsyn. Coll og Lenth har antatt at: «*Personopplysningsloven må trolig forstås slik at dersom den behandlingsansvarlige mener at dette unntaket er nødvendig, så må det gjennomføres overfor alle som i utgangspunktet har rett til informasjon.*»[17] Selv er jeg tvilende til at det eksisterer et slikt «likhetsprinsipp», og at det sentrale er å vurdere hvorvidt unntaket er «påkrevd» opp mot den enkelte registrerte.

6. Må behandlingsansvarlig gi innsyn og informasjon når det ikke lenger er behov for unntak?

Et særlig spørsmål er om informasjonsplikten aktualiseres på nytt når hensynet til hemmelighold ikke lenger gjør seg gjeldende, for eksempel ved avsluttet etterforskning. Det er tenkelig at behandlingsansvarlig da, når unntaket ikke lenger er påkrevd, må informere den registrerte i samsvar med forordningen artiklene 13 og 14.

Departementet fastslo at et «slikt krav ikke [bør] fastsettes uten nærmere utredning, da det vil kunne innebære mye merarbeid for den behandlingsansvarlige». Det ble derfor ikke foreslått en informasjonsplikt i denne omgang. På bakgrunn av dette, har Jarbekk m.fl. antatt at: «Bokstav b inneholder på samme måte etter bokstav a ikke en plikt for den behandlingsansvarlige til å underrette den registrerte når hensynet til hemmelighold ikke lenger gjør seg gjeldende.»[18]

Etter mitt skjønn blir en slik konklusjon for enkel, siden den ikke tar hensyn til forordningens systematikk og adgang til å gi unntak for innsyn og informasjon.[19]

Trolig er adgangen til å gjøre unntak for å ivareta hensynene i bestemmelsen begrenset til tidsperioden det er nødvendig («påkrevd»). Personvernrådet har lagt til grunn at unntak forankret i artikkel 23 nr. 1 bokstav d kun vil gjelde for å ivareta hensynene som begrunner unntak fra informasjonsplikten, og at informasjonsplikten (re)aktiveres så snart etterforskningen mv. ikke lenger kan spoleres:[20]

«[T]he omitted information shall, in accordance with the case law of the CJEU, be provided once and if it is no longer possible for it to jeopardise the investigation being carried out. This means that a specific (tailormade) data protection notice should be given to the data subject as soon as possible, stating the different rights such as access, rectification etc.»

Dette er også i samsvar med EU-domstolens *Opinion 1/15* av 26. juli 2017 om utkast til PNR-avtale mellom Canada og EU.

Ove A. Vanebo, advokat og assosiert partner i CMS Kluge Advokatfirma.

14 Datatilsynets brev av 2. oktober 2009, referansenr. 09/01032-6/CBR.

15 Line M. Coll og Claude A. Lenth, *Personopplysningsloven – en håndbok*, 2000, s. 85.

16 Datatilsynet skriver på sine nettsider at: «Dersom arbeidsgivaren kan undersøkje saka utan å halde varselet hemmeleg, er det ikkje grunnlag for å gjere unntak.»

17 Line M. Coll og Claude A. Lenth, *Personopplysningsloven – en håndbok*, 2000, s. 85.

18 Eva Jarbekk (red.), *Personopplysningsloven og personvernforordningen (GDPR) med kommentarer*, 2019, s. 68.

19 Det kan synes som om dette er en oppfatning som også støttes av Åste Marie Bergseng Skullerud m.fl., *Personopplysningsloven. Lovkommentar*, § 16. Unntak fra retten til informasjon og innsyn og plikten til underretning om brudd på personopplysningssikkerheten, Juridika (kopiert 30. august 2022). Forfatterne viser til at: «*Det kan … anføres at det ikke er nødvendig å pålegge en slik plikt i nasjonal rett, slik departementet synes å legge til grunn.*» Det påpekes videre at «*det ikke bør fastsettes videre unntak enn hva som er nødvendig for å ivareta det hensynet som begrunner unntaket*», og at «*unntaksbestemmelsene skal tolkes med varsomhet, herunder at man skal unngå utvidende tolkning av ordlyden*».

20 Personvernrådet, *Guidelines 10/2020 on restrictions under Article 23 GDPR*, s. 8.

JusNytt

Halvor Manshaus

Leder IP/Media-gruppen i Advokatfirmaet Schjødt AS, Oslo og fast spaltist i Lov&Data.

Nye permanente regler om digitale rettsmøter

Koronapandemien tvang frem en rekke endringer og tilpasninger både for enkeltpersoner, virksomheter og det offentlige. For mange har masken blitt selve bildet på pandemien, men kanskje kunne dette like gjerne vært dataskjermen. Fra full stopp i mars 2020, gikk det raskt over til hjemmekontor og digitale møter. Det er alltid spennende å se hvordan menneskeheten møter store og uventede utfordringer, da må det gjerne gjøres tilpasninger i et hurtig tempo for å ta ned skadevirkningene. I dette tilfellet var det en kombinasjon av en global infrastruktur for kommunikasjon kombinert med stor utbredelse av datamaskiner med video- og lydoverføring som skulle bli redningen. Denne teknologien ble tatt i bruk nærmest umiddelbart, og det som først var en full stopp gikk raskt over til å bli en ny og produktiv arbeidshverdag for millioner av mennesker over hele verden. Skulle det først komme en pandemi var det i dette perspektivet greit at den ikke kom ti år tidligere.

Rettspleien måtte også tilpasses koronatiden, ved at det blant annet ble innført regler om digitale rettsmøter. I stedet for fysiske møter ble det åpnet for at rettsmøter og hovedforhandlinger kunne gjennomføres digitalt. Dette kunne man ha åpnet opp for tidligere, men opplæring og praktisk gjennomføring ville ha vært en stor hindring. Det er bare å tenke tilbake på skolelæreren som skulle spille av noe fra en kassettspiller eller vise noe på overhead. Det fungerte aldri helt som det skulle. Men fordi pandemien i mange tilfeller ikke tillot fysiske møter, var alle aktørene simpelthen nødt til å lære seg å håndtere digitale møter. Igjen så vi hvor tilpasningsdyktige vi egentlig er. En ny digital hverdag som normalt ville ha blitt begrenset av manglende kompetanse og velvillighet hos en rekke av brukerne ble i stedet vårt modus operandi.

Fra egen praksis var det en munter utveksling på kontoret da kollega Halvard Helle skulle i Høyesterett mens advokat Manshaus skulle i en sak for tingretten. Advokat Helle tok heisen til 8. etg og sto på et møterom og prosederte for Høyesterett (skal det først prosederes for Høyesterett skjer det altså ikke sit-

tende – pandemi intet unntak). Saken undertegnede hadde for tingretten gikk i den store ballsalen på Bristol, innleid av tingretten for anledningen for å få tilstrekkelig avstand mellom aktørene. Advokatene Helle og Manshaus prosederte senere under pandemien en sak sammen for Høyesterett, og da hadde vårt advokatkontor også tilpasset seg pandemien. Et auditorium var rigget til med kameraer, talestol og stort lerret. Vi synes vi var kreative da vi la til en tv-skjerm under lerretet der vi kunne ha vår egen disposisjon – som en slags teleprompter.

Etter pandemien sitter vi nå altså igjen med sterk brukerkompetanse og en mer positiv innstilling til digitale møter. I tillegg er det utviklet tekniske løsninger i form av opptaksutstyr og programvare basert på de erfaringene som ble gjort under pandemien. For eksempel vil domstolenes løsning for videolink i dag kunne anvendes av langt flere digitale tilhørere enn tidligere.

Konsekvensen av dette er at Justis- og beredskapsdepartementet i Prop. 97 L (2021-22) fremmet forslag til endringer i straffeprosessloven og tvisteloven som åpnet for større bruk av digitale rettsmøter. De foreslåtte endringene ble innført 3. juni 2022, og trådte i kraft fra 1. juli 2022. De nye permanente reglene avløser de midlertidige reglene fra pandemien. Utgangspunktet vil som tidligere være at rettsmøter gjennomføres fysisk, men åpner i større grad enn tidligere for at rettsmøtene kan gjennomføres digitalt. Det er lagt opp til noe strengere vilkår for digitale rettsmøter i straffesaker grunnet de rettssikkerhetshensyn som gjør seg gjeldende i den type saker. Det er også lagt vekt på at tiltalte og forsvarer skal kunne kommunisere i fortrolighet og uten forstyrrelser.

For sivile saker er det ikke lenger et vilkår at begge partene i saken må samtykke til digitalt rettsmøte. I stedet legger tvisteloven § 13-1 tredje ledd litra b opp til at rettsmøter kan holdes som fjernmøter når dette er «hensiktsmessig og forsvarlig». Partene bør gis anledning til å uttale seg om spørsmålet før retten treffer avgjørelse om eventuelt fjernmøte. Dersom noen av partene motsetter seg fjernmøte skal avgjørelsen avsies ved kjennelse. I vilkåret om at fjernmøtet skal være hensiktsmessig, heter det i forarbeidene at dette må være et bra og effektivt alternativ til et fysisk rettsmøte, blant annet sett hen til kostnader og ulemper forbundet med fysisk fremmøte. Utgangspunktet skal som nevnt være fysiske rettsmøter, og retten må gjøre en konkret vurdering. For partene er det selvsagt viktig å gjøre en vurdering av om saken for deres del er egnet for et fjernmøte, både når det gjelder praktiske hensyn som reisetid og møtets lengde, men også mere praktiske spørsmål knyttet til sakens art. Der det er snakk om kompliserte tekniske spørsmål, eller vurdering av realbevis vil dette kunne tale for at i det minste deler av rettsmøtet gjennomføres fysisk.

Av stor praktisk betydning er den nye hjemmelen for strømming av rettsmøter offentlig, som gir større adgang til domstolene for offentligheten. Fra departementet er det understreket at det fortløpende jobbes med å innføre utstyr for slik strømming av rettsmøter til de rettslokalene som mangler dette i dag.

Som nevnt avløser disse reglene de midlertidige tiltakene fra pandemien. For at det skal være en beredskap knyttet til mulig oppblomstring av korona, er det innført en tidsbegrenset forskriftshjemmel for å innføre tilpasninger til regelverket. Denne hjemmelen opphører 1. januar 2024.

Delphi

Olga Sahlén

I denna notis kommer tre utvalda nyheter från den svenska tillsynsmyndigheten Integritetsskyddsmyndigheten (”IMY”) presenteras.

Tillsyn av Apoteket AB, gällande Facebook-pixel

Tre apotekskedjor har skickat in anmälningar om personuppgiftsincidenter till IMY. Anmälningarna rör personuppgifter som samlats in i företagens webbshoppar och som skickats över till Facebook.

IMY har inlett en tillsyn och nu pågår en granskning. De tre apoteken som är föremål för granskning är Apoteket, Apotea och Apohem.

IMY ställer ett antal frågor till de berörda apotekskedjorna, bland annat vilken typ av personuppgifter som förts över till Facebook, vad syftet med överföringen av uppgifter är, vilken rättslig grund som använts för överföringen och hur bolagen bedömt riskerna med att dela personuppgifter från sina webbshopar med Facebook.

IMY inleder granskning av Kry

Kry International har anmält en personuppgiftsincident som rör överföring av personuppgifter till Facebook. I anmälan framgår att bolaget haft en så kallad Facebook-pixel på två av sina webbplatser vilket medfört att bolaget överfört personuppgifter till Facebook.

IMY inleder således en granskning av det inträffade för att utreda vad som har hänt. Granskningen avser också utreda huruvida Kry anser att bolaget är personuppgiftsansvarig eller personuppgiftsbiträde för överföringen av personuppgifterna.

IMY ställer ett antal frågor till Kry, exempelvis vilka personuppgifter som överförts, hur många personer som kan ha påverkats av incidenten och vilka tekniska och organisatoriska säkerhetsåtgärder bolaget vidtagit.

IMY publicerar nytt rättsligt ställningstagande

Den 27 juni 2022 publicerade IMY ett rättsligt ställningstagande som klargör hur myndigheten tolkar ”undantaget för journalistiska ändamål” som finns i lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen).

I dataskyddslagen finns ett undantag från att följa GDPR då behandling av personuppgifter sker för journalistiska ändamål.

Ställningstagandet behandlar innebörden av begreppet journalistiska ändamål och vad som gäller när det finns andra parallella ändamål.

Begreppet journalistiska ändamål ska enligt IMY ges en bred tolkning och har en bredare innebörd än i vardagligt språkbruk.

Undantaget från skyldigheten att följa GDPR kan omfatta när till exempel privatpersoner sprider information, åsikter eller idéer till allmänheten i sociala medier och således inte endast vad yrkesmässiga journalister och traditionella massmedier gör.

I ställningstagandet anmärks dock att journalistiska ändamål inte kan ges en sådan bred innebörd att det omfattar all information som tillgängliggörs på internet innehållande personuppgifter, exempelvis då en sökmotorleverantör tillhandahåller en sökmotor eller en till allmänheten riktad renodlad söktjänst avseende fällande brottmålsdomar.

Publicering av uppgifter av rent privat karaktär omfattas normalt inte heller av undantaget. Vid en journalistisk granskning av personer i maktposition och då det är nödvändigt att offentliggöra uppgifterna med hänsyn till de journalistiska ändamålen kan dock publicering av rent privata uppgifter omfattas av undantaget för journalistiska ändamål.

I ställningstagandet ger IMY exempel på domstolspraxis av relevans vid tolkningen av begreppet ”journalistiska ändamål”.

IMY ger även tio konkreta exempel på olika typer av

publiceringar av personuppgifter och huruvida dessa omfattas av undantaget för journalistiska ändamål eller inte.

Olga Sahlén, Associate Advokatfirman Delphi Stockholm.


Carl Emil Bull-Berg og Line Helen Haukalid

Bruk av skytjenester – Hvilke spørsmål bør virksomhetene stille seg selv?

Bruk av skytjenester utløser en rekke personvernrettslige plikter. Det er virksomheten som tar i bruk skytjenestene som er behandlingsansvarlig, og som har hovedansvaret for å etterleve personvernregelverket.

Det danske datatilsynet har publisert et spørreskjema som de selv bruker ved tilsyn med private og offentlige aktørers bruk av skytjenester. Spørsmålene dekker sentrale personvernrettslige forpliktelser, og kan derfor fungere som et utgangspunkt for etterlevelse av personvernregelverket også for norske virksomheter.

Det er grunn til å tro at det norske datatilsynet vil stille lignende spørsmål dersom de skulle føre tilsyn med samme eller tilgrensende temaer. I denne artikkelen vil vi derfor med utgangspunkt i spørreskjemaet til det danske datatilsynet oppsummere de viktigste forpliktelsene som den behandlingsansvarlige må overholde i forbindelse med bruk skytjenester.

Hva er skytjenester?

Skytjenester er kort forklart databaserte tjenester som leveres fra eksterne servere via internett. Dette kan være alt fra helt standardiserte produkter som brukes av mange til løsninger som er skreddersydd for den enkelte virksomheten.

De vanligste tjenestemodellene er:

1. Programvare som en tjeneste (software as a service - SaaS), hvor kunden benytter leverandørens ferdigutviklede nettbaserte applikasjoner. Leverandøren har ansvaret for drift og vedlikehold, og kundens kontroll over applikasjoner, nettverk, operasjonssystemer og lagringsmuligheter er svært begrenset.
2. Plattform som en tjeneste (platform as a service – PaaS), hvor kunden benytter leverandørens infrastruktur og eventuelle tilhørende verktøy og funksjoner. Her kan kunden implementere egne eller kjøpte applikasjoner. Kunden har kontroll over implementerte applikasjonene og innstillinger, men har ikke kontroll over nettverk, servere, operativsystemer eller lagringsmuligheter.
3. Infrastruktur som en tjeneste (infratructure as a service – IaaS), hvor kunden kjøper ren infrastruktur og implementerer all software, herunder operativsystemer og applikasjoner. Kunden har kontroll over applikasjoner, nettverk, servere, operativsystemer og lagringsmuligheter, og står selv for drift og vedlikehold.

Viktigheten av risikovurderinger

Allerede før man går til anskaffelse av en skytjeneste stiller personvernregelverket krav til den behandlingsansvarlige. GDPR krever at den behandlingsansvarlige foretar en risikovurdering av tjenesten. I dette ligger blant annet at den behandlingsansvarlige må vite hvilke personopplysninger som skal behandles i tjenesten, hvilke tiltak som er implementert for å oppnå tilfredsstillende informasjonssikkerhet, hvilke leverandører og underleverandører som får tilgang til personopplysningene og om personopplysningene vil bli behandlet i land utenfor EØS.

Risikovurderinger er også et sentralt element i spørreskjemaet til det danske datatilsynet. Tilsynet ber blant annet den behandlingsansvarlige redegjøre for om det er gjennomført en risikovurdering av skytjenesten før tjenesten er tatt i bruk og om eventuelle rutiner for gjennomføring av risikovurderinger. Det stilles spørsmål både til risikovurdering av selve skytjenesten og av leverandøren.

Screening av leverandøren

Leverandøren av skytjenester vil normalt behandle kundens personopplysninger som en databehandler. Det følger av GDPR artikkel 28(1) at den behandlingsansvarlige kun

kan bruke databehandlere som gir tilstrekkelige garantier for at de vil behandle personopplysningene i tråd med personvernregelverket. For å forsikre seg om at dette er tilfellet, må den behandlingsansvarlige foreta en screening (risikovurdering) av leverandøren. GDPR legger ingen føringer for hvordan denne screeningen skal gjennomføres. I spørreskjemaet finnes imidlertid en viss veiledning. Den behandlingsansvarlige blir blant annet bedt om å svare på om følgende er hensyntatt i screeningen:

- Om leverandøren behandler kundens personopplysninger for egne formål
- Om det er inngått databehandleravtale med leverandøren som oppfyller kravene i GDPR
- Om leverandøren har etablert et egnet sikkerhetsnivå, i lys av den aktuelle behandlingsaktiviteten
- Kartlegging av alle underdatabehandlere og rutiner for å sørge for at nødvendige (under)databehandleravtaler er på plass
- Leverandørens rutiner for risikovurderinger av underdatabehandlere for å sikre at også disse har etablert et egnet sikkerhetsnivå.
- Leverandørens rutiner for å dokumentere at underdatabehandlerne har et egnet sikkerhetsnivå
- Leverandørens rutiner for å bistå den behandlingsansvarlige med håndtering av de registrertes rettigheter
- Leverandørens rutiner for varsling og bistand ved eventuelle sikkerhetsbrudd
- Muligheter for sikkerhetsrevisjoner av leverandøren
- Om leverandøren er i stand til å overholde plikten til å slette eller tilbakelevere personopplysningene ved opphør av avtalen
- Overføringer av tredjeland i strid med den behandlingsansvarliges instrukser

Merk at valg av tjenestemodell påvirker risikovurderingen den behandlingsansvarlige må gjennomføre. Jo flere oppgaver som settes ut til leverandøren, desto grundigere må risikovurderingen være.

Plikt til å revidere leverandøren av skytjenestene

Selv om man har foretatt en forsvarlig risikovurdering av skytjenesteleverandøren og konkludert med at leverandøren gir slike tilstrekkelige garantier som loven krever, opphører ikke plikten til å forsikre seg om at personopplysningene behandles forsvarlig i skytjenesten. Et nyttig virkemiddel i den forbindelse er sikkerhetsrevisjoner. Den behandlingsansvarlige har plikt til å sørge for at databehandleravtalen gir rett til revisjon av skytjenesteleverandøren.

I spørreskjemaet stiller det danske datatilsynet flere spørsmål om utøvelse revisjonsretten. Herunder må den behandlingsansvarlige redegjøre for om det er etablert rutiner for gjennomføring av sikkerhetsrevisjoner, og om disse inneholder retningslinjer for hyppigheten av slike revisjoner, håndtering av eventuelle avvik og terminering av avta-

len ved større avvik, samt kontroll av leverandørens etterlevelse av personvernregelverket ved eventuelle lovendringer. Disse spørsmålene viser blant annet at datatilsynet forventer at man med jevne mellomrom faktisk gjennomfører sikkerhetsrevisjoner, særlig der behandlingens art og omfang tilsier høy personvernrisiko. I tillegg vil nok også valg av tjenestemodell kunne påvirke hyppigheten og omfanget av slike personvernrevisjoner.

Overføring av personopplysninger til tredjeland

Mange eksterne serverparker befinner seg utenfor EØS. Etter EU-domstolens avgjørelse i Schrems II-saken og etterfølgende veiledere fra the European Data Protection Board (EDPB) stilles skjerpede krav for at en overføring av personopplysninger til et tredjeland skal være lovlig. Det danske datatilsynet stiller en rekke spørsmål knyttet til eventuelle internasjonale dataoverføringer for å kontrollere at retningslinjene til EDPB er fulgt opp. Nærmere bestemt, må den behandlingsansvarlige redegjøre for sine kartlegginger av slike overføringer og tilhørende rutiner. I tillegg stilles blant annet spørsmål om overføringsgrunnlag, vurderinger av beskyttelsesnivået i tredjelandet og eventuelle ytterligere beskyttelsestiltak.

Viktigheten av rutiner

Gjennomgående i spørreskjemaet er at det danske datatilsynet stiller spørsmål om den behandlingsansvarliges dokumenterte interne personvernrutiner og -prosedyrer. De påpeker samtidig at det ikke gjelder et absolutt krav om å etablere slike rutiner og prosedyrer, men at dette er et nyttig redskap ved bruk av skyløsninger.

Det stemmer at ikke alle virksomheter/behandlingsansvarlige må ha formaliserte interne rutiner. Dette følger forutsetningsvis av GDPR artikkel 24(2), som viser til at den behandlingsansvarliges tekniske og organisatoriske tiltak skal omfatte egnede retningslinjer dersom det står i et rimelig forhold til behandlingsaktivitetene. Mange virksomheter vil imidlertid ha behandlingsaktiviteter av en slik art og omfang at det nettopp er et krav om formaliserte retningslinjer og rutiner for å sikre at personvernet ivaretas. Uten slike rutiner vil det dessuten være utfordrende å dokumentere etterlevelse av personvernregelverket i tråd med ansvarlighetsprinsippet i GDPR artikkel 5(2).

Oppsummering

Kort oppsummert, stilles det strenge krav til risikovurderinger og oppfølging av leverandøren når man tar i bruk en skytjeneste. Som nevnt innledningsvis, er det grunn til å tro at det norske datatilsynet vil stille lignende spørsmål ved eventuelle tilsyn. Selv om spørreskjemaet er spesifikt rettet mot skytjenester, er forpliktelsene som spørsmålene gjelder generelle, og kommer til anvendelse ved kjøp av de fleste tjenester som innebærer behandling av personopplysninger. Spørreskjemaet kan derfor fungere som en nyttig sjekkliste i videre compliance-arbeid.

Line Helen Haukalid er fast advokat i Advokatfirmaet Wiersholm.
Carl Emil Bull-Berg er associates i Advokatfirmaet Wiersholm.

Gorrissen Federspiel

Tue Goldschmieding

Kommissionen sætter en stopper for dansk lovforslag om en strammere regulering af sociale medier

Det danske Erhvervsministerium udsendte den 29. marts 2022 nyhed om et lovforslag vedrørende skærpede krav til sociale medier og ulovligt indhold på platformene. EU-Kommissionen blokerede dog forslaget, da lignende regler er foreslået af Kommissionen ved Europa-Parlamentets forslag til forordning om et indre marked for digitale tjenester (retsakt om digitale tjenester) og om ændring af direktiv 2000/31/EF af 8. maj 2001. Blokeringen skyldes, at Kommissionen ikke vil acceptere, at de danske regler træder i kraft før forordningen.

Det danske forslag indebar, at det skulle være nemt for brugerne at anmelde ulovligt indhold på platformene. Anmeldelsen skulle behandles inden for 24 timer og begrundes over for brugeren, hvis indholdet blev fjernet. Derudover skulle beslutningen om at fjerne indhold fra platformen kunne efterprøves, såfremt brugeren, der fik fjernet indholdet, var uenig i beslutningen. Endelig skulle virksomheden afgive en gennemsigtighedsrapport én gang årligt. Manglende overholdelse af reglerne ville medføre bødestraf.

Det danske forslag stemte i høj grad overens med forordningen, da denne tillige medfører større krav til fjernelse af ulovligt indhold, større gennemsigtighed fra virksomhederne og klageadgang for den bruger, der har fået fjernet indhold. Det danske forslag fraveg forordningen ved at fastsætte en bestemt tidsgrænse for, hvornår ulovligt indhold skulle tages ned.

De danske regler ville være trådt i kraft hhv. den 1. juli 2022 og 1. september 2022, hvorimod det er uklart, hvornår EU-reglerne træder i kraft. Dele af forordningen træder tidligst i kraft i løbet af 2023 og resten i 2024.

Læs pressemeddelelsen her: https://em.dk/nyhedsarkiv/2022/maj/eu-kommissionen-bremser-danske-ambitioner-om-strammere-krav-til-sociale-medier/

Læs om lovforslaget her: https://em.dk/nyhedsarkiv/2022/marts/ny-lovgivning-skal-skaerpe-kravene-til-sociale-medier/

Kommissionen har stillet forslag til en forordning om det europæiske sundhedsområde

Den 3. maj 2022 fremsatte EU-Kommissionen forslag om at etablere et europæisk sundhedsdataområde (EHDS). Forordningen skal ses som led i Kommissionens ønske om at opbygge en europæisk sundhedsunion. Hovedformålet med forslaget er at sikre, at fysiske personer i EU har større kontrol med deres elektroniske sundhedsdata.

På baggrund af covid-19-pandemien, anså Kommissionen det for nødvendigt at regulere sundhedsområdet for at sikre rettidig adgang til sundhedsdata i forbindelse med beredskab og indsats over for sundhedstrusler samt behandling under sundhedskriser. Forslaget fremmer det indre marked for sundhedsydelser ved at muliggøre, at sundhedsdata nemmere kan udveksles mellem sundhedspersonalet i og på tværs af EU-landene ligesom, at denne data kan anvendes på en pålidelig og sikker måde af forskere, innovatorer og politiske beslutningstagere. Derudover får EU-borgerne mulighed for at kontrollere og korrigere deres elektroniske sundhedsdata i deres hjemland samt i andre medlemsstater. Det følger af forslaget til forordningen, at medlemsstaterne skal udpege en digital sundhedsmyndighed, der skal sikre, at borgernes rettigheder beskyttes.

Forslaget bidrager til, at reglerne på sundhedsområdet harmoniseres, hvilket vil være med til at øge sundhedsvæsenets effektivitet i medlemsstaterne.

Læs hele pressemeddelelsen her: https://ec.europa.eu/commission/presscorner/detail/da/ip_22_2711

Læs hele forslaget til forordningen her: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197

Ny EDPB-vejledning om databeskyttelse på sociale medier

Det Europæiske Databeskyttelsesråd (EDPB) vedtog den 14. marts 2022 en vejledning om databeskyttelse på sociale medier. Denne vejledning omhandler sociale mediers databehandling i såkaldte »interfaces«. Interfaces kendes også som »dark patterns« og vedrører en række fremgangsmåder, som visse sociale medier anvender i forbindelse med databehandling af registreredes oplysninger, når de opretter en brugerprofil.

Et eksempel på »dark patterns« kan være, hvis det sociale medie forsøger følelsesmæssigt at påvirke den

registrerede til at træffe bestemte valg for så vidt angår behandlingen af deres personoplysninger. »Dark patterns« kan også være »overloading«, hvor virksomheden præsenterer brugeren for uforholdsmæssigt meget information således, at der forsøges at indsamle flere oplysninger end hvad der er nødvendigt i forhold til formålet i forbindelse med oprettelse af en brugerprofil på virksomhedens sociale medie.

Vejledningen er relevant i forbindelse med dataansvarliges tilrettelæggelse forinden iværksættelse af behandling af personoplysninger, herunder eventuelle designmæssige foranstaltninger, der skal indføres på sociale medier. Den er ligeledes relevant i forbindelse med behandling af personoplysninger om hjemmesidebesøgende, hvor en udformning af en samtykkeløsning eller anden fremgangsmåde benyttes til at behandle personoplysningerne. Her skal den dataansvarlige på samme måde undgå at bruge »dark patterns« til at skubbe en bruger eller besøgende i retning af et bestemt valg når det kommer til den databehandling der foregår, når man som bruger besøger en hjemmeside.

»Dark patterns« har således stor betydning for allerede registrerede brugere og fremtidige brugere på sociale medier.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/internationalt/internationalt-nyt/2022/mar/ny-edpb-vejledning-om-databeskyttelse-i-interfaces-paa-sociale-medier

Læs EDPBs pressemeddelelse her: https://edpb.europa.eu/news/news/2022/edpb-adopts-guidelines-art-60-gdpr-guidelines-dark-patterns-social-media-platform_en

Det Europæiske Databeskyttelsesråd (EDPB) har vedtaget en ny fælleseuropæisk bødevejledning

Det Europæiske Databeskyttelsesråd (EDPB) vedtog den 12. maj 2022 en ny fælleseuropæisk bødevejledning.

Bødevejledningen, der blev udarbejdet i gruppen Task Force Fining, uddyber selve fremgangsmåden ved bødeberegningen vedrørende reglerne om Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«).

Retningslinjerne, der skal harmonisere praksis for bødeberegningen i hele Det Europæiske Økonomiske Samarbejdsområde, indeholder en beregningsmetode bestående af fem trin.

For det første skal databeskyttelsesmyndighederne fastslå, om den pågældende sag vedrører et tilfælde af strafbar adfærd, og om de har ført til en eller flere overtrædelser. Derved afklares, hvilke overtrædelser der kan pålægges bøder for.

For det andet baserer databeskyttelsesmyndighederne beregningen af bøden på et udgangspunkt, som EDPB nu giver en harmoniseret metode for.

For det tredje skal databeskyttelsesmyndighederne tage hensyn til skærpende eller formildende faktorer, der kan øge eller mindske bødens størrelse. EDPB giver en ensartet fortolkning af disse faktorer.

Det fjerde trin er, at fastsætte maksimumsbeløb for bøder som fastsat i GDPR art. 83, stk. 4-6, og at sikre, at disse beløb ikke overskrides.

Som det femte og sidste trin, skal databeskyttelsesmyndighederne vurdere, om det endelige beløb opfylder kravene om effektivitet, afskrækkende virkning og proportionalitet, eller om der er behov for yderligere justeringer af beløbet.

Retningslinjerne er et vigtigt supplement til de rammer, som EDPB er ved at opbygge for et mere effektivt og harmoniseret samarbejde mellem de nationale databeskyttelsesmyndigheder.

Retningslinjerne sendes til offentlig høring i en periode på seks uger, hvorefter en endelig version af retningslinjerne, under hensyntagen til tilbagemeldinger fra de hørte parter, vedtages.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/internationalt/internationalt-nyt/2022/maj/ny-faelleseuropaeisk-boedevejledning

Læs EDPBs pressemeddelelse her: EDPB adopts Guidelines on calculation of fines & Guidelines on the use of facial recognition technology in the area of law enforcement | European Data Protection Board (europa.eu)

Læs hele vejledningen her: https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf

Ny EDPB-vejledning om brug af certificering som overførselsgrundlag

Den 14. juni 2022 vedtog Det Europæiske Databeskyttelsesråd (»EDPB«) en vejledning med henblik på offentlig høring, om brugen af certificeringsordninger som grundlag for overførsel af personoplysninger til et tredjeland eller en international organisation i henhold til Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 46, stk. 2, litra f.

EDPB har tidligere offentliggjort generelle vejledninger vedrørende certificering og akkreditering under GDPR. Hovedformålet med den nye vejledning er derfor at skabe yderligere klarhed om den praktiske anvendelse af certificeringsordninger som overførelsesgrundlag. EDPB vejleder således om de specifikke aspekter af certificering som et værktøj til overførelser, når der ikke foreligger en tilstrækkelighedsafgørelse.

Vejledningen omfatter oprettelsen af en certificeringsordning for dataimportører, dataansvarlige og databehandlere fra tredjelande i forbindelse med én eller flere behandlinger. Certificeringen vil gøre det muligt for disse dataimportører at påvise, at der eksisterer passende sikkerhedsforanstaltninger til at imødegå de specifikke risici, der er forbundet med overførsel af personoplysninger

fra enheden baseret i EØS. Ifølge vejledningen er dataeksportøren i EØS ansvarlig for at sikre, at dataimportørens certificering er effektiv i lyset af karakteristika for den påtænkte behandling og den gældende lov og praksis i tredjelandet. Vejledningen nævner specifikt, at dataeksportøren bør kontrollere, at der foreligger en kontrakt eller et andet juridisk bindende dokument mellem den certificerede dataimportør og certificeringsorganet.

Vejledningen er sendt til offentlig høring indtil udgangen af september 2022, hvorefter EDPB i lyset af de indkomne høringssvar vil vurdere behovet for eventuelle ændringer, før vejledningen endeligt vedtages.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/internationalt/internationalt-nyt/2022/jun/edpb-vedtager-vejledning-om-brug-af-certificering-som-overfoerselsgrundlag

Læs EDPBs pressemeddelelse her: https://edpb.europa.eu/news/news/2022/edpb-adopts-guidelines-certification-tool-transfers-and-art-65-dispute-resolution_lt

Læs hele vejledningen her. edpb_guidelines_202207_certificationfortransfers_en_1.pdf (europa.eu)

Datatilsynet redegør for begrebet »dataeksportør«

Det danske Datatilsyn udsendte den 8. juni 2022 nyhed om, at Datatilsynet har udarbejdet en kort vejledende tekst, der redegør for tilsynets vurdering af begrebet »dataeksportør«.

Redegørelsen udspringer af, at tilsynet har modtaget et stigende antal spørgsmål vedrørende overførsel af personoplysninger til tredjelande i lyset af EU-Domstolens dom i sag C-311/18, Screms II, som vedrørte brugen af EU-Kommissionens standardkontrakter og EU US Privacy Shield.

Vejledningen har til formål at redegøre for tilsynets vurdering af, hvem der i praksis er ansvarlig for at sikre, at overførsel af personoplysninger til tredjelande er lovlig, når overførslen sker på baggrund af Kommissionens standardkontrakt.

Tilsynet vurderer, at Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 44, som indeholder det generelle princip for overførsel af personoplysninger til tredjelande, er en forpligtelse for både den dataansvarlige og databehandleren. Således er begge parter forpligtet til at sørge for, at der tilvejebringes et overførselsgrundlag, der er effektivt i lyset af alle omstændighederne ved overførslen.

Det gælder i praksis også i de tilfælde, hvor databehandleren har indgået en standardkontrakt med eventuelle underdatabehandlere i tredjelande i henhold til GDPR artikel 46, stk. 2, litra c, der hjemler brugen af standardbestemmelser om databeskyttelse vedtaget af Kommissionen. Den dataansvarlige skal herefter sikre sig, og kunne påvise over for Datatilsynet, at databehandleren har etableret det fornødne overførselsgrundlag, og at dette overførselsgrundlag er effektivt i lyset af alle omstændighederne ved overførslen, herunder om nødvendigt ved implementering af supplerende foranstaltninger.

Læs pressemeddelelsen her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/jun/om-begrebet-%e2%80%9ddataeksportoer%e2%80%9d

Læs den vejledende tekst her: https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/cloud/om-begrebet-dataeksportoer

Står det i databehandleraftalen, er det ikke en utilsigtet overførsel

Kort efter at det danske Datatilsyn den 9. marts 2022 udgav en vejledning om brugen af cloud services henvendte virksomheden KOMBIT sig til Datatilsynet med et konkret spørgsmål foranlediget af vejledningens afsnit om udlevering af oplysninger til myndigheder i tredjelande.

KOMBIT leverer systemet Aula til de danske kommuner, og benytter i den forbindelse underleverandøren Netcompany, som yderligere benytter Amazon Web Services som underleverandør. KOMBIT behandler som udgangspunkt personoplysninger inden for EU/EØS, men af databehandleraftalen mellem Netcompany og Amazon Web Services fremgår, at dette kan fraviges i to tilfælde. For det første, hvis det er nødvendigt for leveringen af visse specifikke AWS services valgt af servicebrugeren og for det andet, hvis det er nødvendigt for at overholde lovgivning eller bindende myndighedsanmodninger.

Det konkrete spørgsmål var, hvorvidt der var tale om en utilsigtet eller tilsigtet overførsel, i det tilfælde muligheden for overførsel af personoplysninger til myndigheder i tredjelande fremgår af databehandlerens standarddatabehandleraftale.

Det var Datatilsynets opfattelse, at der ville være tale om en tilsigtet overførsel af personoplysninger til tredjelande for kommunernes vedkommende, hvis og i det omfang Amazon Web Services imødekommer en anmodning fra en offentlig myndighed i et tredjeland, der omfatter personoplysninger, som kommunerne er dataansvarlige for. I den forbindelse fremhævede Datatilsynet, at kommunerne som dataansvarlig skal sikre, at reglerne om overførsler til tredjelande overholdes, når eller hvis Amazon Web Services foretager en sådan overførsel i henhold til den instruks, der fremgår af databehandleraftalen. Endvidere lagde datatilsynet op til en videre dialog om den nævnte problemstilling.

Læs pressemeddelelsen her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/apr/staar-det-i-databehandleraftalen-er-det-ikke-utilsigtet

Læs hele Datatilsynets svar her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/mar/vedroerende-tilsigtede-eller-utilsigtede-overfoersler-til-tredjelande

For første gang straffes en dansk offentlig myndighed for overtrædelse af GPDR-reglerne

Retten i Roskilde har den 9. marts 2022 idømt Lejre Kommune til at be-

tale en bøde på 50.000 kr. på baggrund af manglende betalingssikkerhed.

Sagen blev politianmeldt af det danske Datatilsyn tilbage i juni 2020 og vedrører en overtrædelse af Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 32 om passende tekniske og organisatoriske sikkerhedsforanstaltninger. Den konkrete sag drejede sig om, at Lejre Kommunes praksis om, at møde-referater, der indeholdte personoplysninger med særlig følsom karakter, herunder om borgere under 18 år, blev uploadet på kommunens medarbejderportal. Dette medførte, at en stor del af kommunens ansatte havde adgang til referaterne, uagtet at de ikke arbejdede med den type sager. Kommunen levede dermed ikke op til kravene om passende sikkerhedsforanstaltninger.

Retten lagde særligt vægt på omfanget samt karakteren af de følsomme oplysninger. Samtidig blev der lagt vægt på antallet af personer, der havde haft uberettiget adgang til oplysningerne over en længere periode.

Retten idømte på denne baggrund Lejre Kommune en bøde på 50.000 kr. Denne bøde stemmer overens med det beløb som Datatilsynet havde indstillet i forbindelse med politianmeldelsen.

Dommen findes særligt interessant, idet den udgør den første dom, hvor en dansk offentlig myndighed straffes for overtrædelse af de databeskyttelsesretlige regler.

Læs pressemeddelelsen her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/mar/foerste-gdpr-boede-til-offentlig-myndighed

Datatilsynet meddeler advarsel til Fysio Danmark Hillerød ApS i en sag om påtænkt anvendelse af ansigtsgenkendelsessystem

Det danske Datatilsyn traf den 17. marts 2022 afgørelse i sagen 2021-431-0145 vedrørende en virksomheds påtænkte brug af et system til ansigtsgenkendelse.

Datatilsynet vurderede i sagen, hvorvidt Fysio Danmark Hillerød ApS' (»Fysio Danmark«) påtænkte anvendelse af et ansigtsgenkendelsessystem var i overensstemmelse med reglerne i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«)

Fysio Danmark påtænkte at anvende et ansigtsgenkendelsessystem til både kunder og ansatte, der udtrykkeligt havde samtykket hertil. Ansigtsgenkendelsessystemet skulle bruges som adgangskontrol, samt til statistik og forretningsoptimering ved behandling af oplysninger om kundernes opholdstider i fitnesscenteret. For kunder eller ansatte, der ikke ønskede at give samtykke til ansigtsgenkendelsessystemet, var det muligt at få adgang til fitnesscenteret ved andre løsninger.

Datatilsynet vurderede, at det ikke var i strid med GDPR at bruge ansigtsgenkendelsessystemet for kunder og ansatte, der havde givet et udtrykkeligt og frivilligt samtykke. Vedrørende frivilligheden af de ansattes samtykke, lagde Datatilsynet særligt vægt på, at der tilbydes andre adgangsløsninger, samt at det alene er den ansattes ankomsttid der registreres, hvorimod der ikke lagres oplysninger om, hvornår den ansatte forlader arbejdspladsen.

Vedrørende brugen af ansigtsgenkendelsessystemet til forretningsoptimering vurderede Datatilsynet, at det ville være i strid med GDPR, hvis kunden ikke har givet udtrykkeligt samtykke hertil. Idet den nuværende samtykkeløsning ikke levede op til dette, meddelte Datatilsynet Fysio Danmark en advarsel efter GDPR artikel 58, stk. 2, litra a.

Datatilsynet tildelte ligeledes en advarsel for anvendelsen af ansigtsgenkendelsessystemet, da der ved den påtænkte måde ville blive behandlet biometriske data om personer, der ikke havde givet samtykke.

Læs pressemeddelelsen her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/mar/datatilsynet-har-truffet-afgoerelse-i-en-sag-om-brugen-af-et-system-til-ansigtsgenkendelse

Læs hele afgørelsen her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/mar/datatilsynet-har-truffet-afgoerelse-i-en-sag-om-brugen-af-et-system-til-ansigtsgenkendelse

Danske Bank politianmeldes og indstilles til bøde på DKK 10 mio. grundet manglende sletning

Den 5. april 2022 meddelte Det danske Datatilsyn, at Danske Bank var blevet anmeldt til politiet og indstillet til en bøde på DKK 10 mio. af Datatilsynet for ikke at kunne dokumentere, at de har slettet personoplysninger i overensstemmelse med databeskyttelsesreglerne.

Politianmeldelsen og indstillingen til bøde skete på baggrund af, at Datatilsynet i november 2020 indledte en sag af egen drift, efter at Danske Bank havde oplyst, at de havde identificeret et problem med sletning af personoplysninger. Datatilsynets undersøgelse påviste, at Danske Bank i mere end 400 systemer ikke havde kunnet dokumentere, at der var fastsat regler for sletning og opbevaring af personoplysninger om flere millioner registrerede, eller at der var foretaget manuel sletning af personoplysninger.

Datatilsynet lagde vægt på, at der bør idømmes en bøde, idet overtrædelsen vedrører et grundlæggende princip for behandling af personoplysninger, nemlig at man kun må behandle oplysninger, man har brug for, ligesom behandlingen berører et meget stort antal registrerede.

Læs pressemeddelelsen her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/apr/danske-bank-indstilles-til-boede

Gyldendal politianmeldt for at opbevare oplysninger om over 650.000 tidligere medlemmer i længere tid end nødvendigt

Det danske Datatilsyn udsendte den 22. juni 2022 en nyhed om, at Datatilsynet efter et tilsynsbesøg hos Gyldendal A/S har anmeldt virksomhe-

den til politiet og indstillet forlaget til en bøde på 1.000.000 mio. kr. Anmeldelsen kommer på baggrund af, at Gyldendal har opbevaret oplysninger om ca. 685.000 udmeldte medlemmer af Gyldendals bogklub i længere tid end nødvendigt.

Oplysningerne blev opbevaret i en »passiv database«, hvortil Gyldendal ikke havde procedurer eller retningslinjer for sletning af oplysningerne. Oplysninger om ca. 395.000 af de tidligere medlemmer var blevet opbevaret i mere end 10 år efter, at medlemmerne havde meldt sig ud af bogklubberne.

Opbevaringen er efter tilsynets opfattelse i strid med to grundlæggende principper for behandling af personoplysninger, nemlig principperne om »opbevaringsbegrænsning« og »ansvarlighed«. Herudover berører overtrædelsen et meget stort antal registrerede. Datatilsynet fandt på denne baggrund grundlag for at indstille Gyldendal til en bøde efter Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 83, stk. 2, hvorefter der skal foretages en konkret vurdering af sagens grovhed ved vurderingen af, hvilken sanktion, der er mest hensigtsmæssig.

Tilsynet har ved vurderingen af bødens omfang i skærpende retning lagt vægt på, at der var tale om et grundlæggende problem, frem for en enkeltstående fejl samt at overtrædelsen efter tilsynets vurdering er begået forsætligt. Det har derimod i formildende retning bl.a. været tillagt vægt, at Gyldendal har ageret særdeles samarbejdsvillig, og at der ifølge Gyldendal alene var to medarbejdere, der havde adgang til den passive database.

Læs pressemeddelelsen her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/jun/gyldendal-indstilles-til-boede

Datatilsynet udtaler kritik af e-Boks for utilstrækkelig sikkerhed i e-Boks Express

Det danske Datatilsyn traf den 3. marts 2022 afgørelse i sagen 2021-431-0138 vedrørende manglende sikkerhed i selvbetjeningsportalen e-Boks Express.

I marts 2021 startede Datatilsynet af egen drift en sag mod e-Boks, efter man var blevet gjort opmærksom på, at der var sket et databrud hos selvbetjeningsportalen.

Databruddet skyldtes en fejlopsætning i Nets' brugervalidering, hvilket resulterede i, at det var muligt for brugere af portalen at tilgå andre brugeres profiler. Databruddet omfattede alene de tilfælde, hvor en bruger tilgik e-Boks Express med medarbejdersignatur, dvs. nøglekort eller nøgleapp.

Datatilsynet vurderede, at e-Boks ikke havde truffet passende sikkerhedsforanstaltninger, ved ikke at have

foretaget test af alle relevante brugsscenarier ved login i e-Boks Express med NemID, og kom frem til, at e-Boks sikkerhedsniveau var i strid med Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 32, stk. 1.

På baggrund af ovenstående udtalte Datatilsynet kritik af e-Boks' manglende sikkerhedsforanstaltninger. Datatilsynet lagde herved særligt vægt på, at fejlfindingsprocedurer ligeledes skal afdække mulige fejlscenarier i den valgte log-on komponent.

I formildende retning lagde Datatilsynet vægt på, at det udelukkende var muligt at se den anden profils virksomhedsnavn, titlen på afsendte beskeder og afsendelsestidspunktet for beskederne.

Læs pressemeddelelsen her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/mar/-e-boks-faar-kritik-for-ikke-at-have-passende-sikkerhed

Læs hele afgørelsen her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/mar/e-boks-faar-kritik-for-ikke-at-have-passende-sikkerhed

Digitaliseringsstyrelsen får kritik for at basere sin sikkerhed på, at der ikke tidligere er sket menneskelige fejl

Det danske Datatilsyn traf den 4. marts 2022 afgørelse i sagen 2021-442-12425 vedrørende manglende sikkerhedsforanstaltninger hos den danske Digitaliseringsstyrelse.

Den 31. marts 2021 meddelte Digitaliseringsstyrelsen, at der var sket et brud på persondatasikkerheden. I forbindelse med tildeling af kuratoradgang til virksomheders digitale postkasser, havde Digitaliseringsstyrelsen fejlagtigt forskudt linjerne på CVR-numrene på den relevante liste. Adgangshaverne og adgangsgiverne var således sammensat forkert. Der var sket i alt 26 brud på datasikkerheden af ovenstående karakter.

Datatilsynet vurderede, at Digitaliseringsstyrelsen ikke havde truffet passende tekniske og organisatoriske sikkerhedsforanstaltninger. Begrundelsen herfor var, at Digitaliseringsstyrelsen alene havde baseret sikkerhedsniveauet på, at der ikke før var sket menneskelige fejl af samme karakter.

På baggrund af ovenstående udtalte Datatilsynet kritik af Digitaliseringsstyrelsen for ikke at overholde Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 32, stk. 1, som netop omhandler indretningen af et passende sikkerhedsniveau.

Digitaliseringsstyrelsen har efterfølgende justeret deres procedurer, ved at implementere et flerøjneprincip ved tildeling af kuratoradgang til virksomhedspostkasserne.

Læs pressemeddelelsen her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/mar/-digitaliseringsstyrelsen-faar-kritik-for-ikke-at-have-haft-passende-sikkerhed-

Læs hele afgørelsen her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/mar/digitaliseringsstyrelsen-faar-kritik-for-ikke-at-have-haft-passende-sikkerhed

Dataansvarlige skal føre kontrol med, om der ved en fejl er gemt personoplysninger i it-miljøer, selvom disse ikke må bruges til opbevaring af personoplysninger

Det danske Datatilsyn traf den 16. marts 2022 afgørelse i sagen 2021-442-12991 vedrørende manglende kontrol med lagring af personoplysninger i visse it-miljøer.

Den danske Sundhedsdatastyrelse meddelte i maj 2021, at der var sket et brud på persondatasikkerheden. En tidligere medarbejder havde fejlagtigt gemt et dataudtræk indeholdende pseudonymiserede helbredsoplysninger i programmet Microsoft Aure DevOps, som blev brugt til opgavestyring. Programmet udgjorde således ikke et it-miljø, hvor persondata normalt blev lagret. Af samme årsag, havde sundhedsdatastyrelsen ikke indrettet nogle mekanismer til at kontrollere miljøet for lagrede persondata.

Datatilsynet vurderede på den baggrund, at Sundhedsdatastyrelsen ikke havde etableret et passende sikkerhedsniveau, idet man ikke havde ført tilstrækkelig kontrol med visse it-miljøer.

Ved vurderingen lagde Datatilsynet særligt vægt på, at der var tale om en stor mængde personoplysninger om forskellige borgere fra region Hovedstaden, og at der gik ca. et år før sikkerhedsbruddet blev meddelt.

I formildende retning vurderede Datatilsynet, at personoplysningerne havde været pseudonymiseret og kun var tilgængelige for enkelte særlige medarbejdere.

På baggrund af ovenstående udtalte Datatilsynet kritik af, at Sundhedsdatastyrelsens kontrol med behandlingen af personoplysninger er i strid med reglerne i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 32, stk. 1, om passende tekniske og organisatoriske sikkerhedsforanstaltninger.

Læs pressemeddelelsen her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/mar/sundhedsdatastyrelsen-faar-kritik-for-manglende-kontrol-med-personoplysninger-i-it-miljoe

Læs hele afgørelsen her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/mar/sundhedsdatastyrelsen-faar-kritik-for-manglende-kontrol-med-personoplysninger-i-it-miljoe

Tue Goldschmieding er partner i Gorrissen Federspiel og en av de danske redaktørene for Lov&Data.

simonsen vogtwiig

Hedda Baumann Heier og Emile Schjønsby-Nolet

Høyesterett med avklaringer om medias bruk av verk

Den 2. juni 2022 publiserte Høyesterett sin avgjørelse i sak med saksnummer HR-2022-1113-A mellom Advokatfirmaet Rogstad AS («Rogstad») og avisen Verdens Gang AS («VG»). Konflikten oppstod da VG i en serie kritiske nyhetsartikler publiserte fotografier fra advokatfirmaets nettside og facebookprofilen til én av advokatfirmaets ansatte uten samtykke. Partene var i saken enige om at bildene var fotografiske bilder beskyttet etter åndsverkloven («åvl») § 23. Utgangspunktet er da at det kreves samtykke for å publisere fotografiene. Tvistespørsmålet i saken var om bruken var hjemlet i en av unntak-/avgrensningsreglene i åndsverksloven, henholdsvis i sitatregelen i § 29 (sitatregelen) eller tvangslisensen i § 36 andre ledd for bruk av fotografiske verk som har tilknytning til en dagshending uten å inngå i den.

Høyesterett tok først stilling til forholdet mellom åvl §§ 29 og 36 andre ledd. Selv om begge reglene er hjemlet i kapittel 3, er sitatretten i åvl § 29 en såkalt «fribruksregel» som ikke forutsetter vederlag for bruk. Motsetningsvis kan opphaver kreve vederlag for bruk hjemlet i tvangslisensen i § 36 andre ledd. Spørsmålet var om de to bestemmelsene utgjør selvstendige avgrensningsregler uten noen innbyrdes sammenheng eller om § 36 annet ledd er en spesialregel som går foran § 29 og skal anvendes så langt vilkårene i bestemmelsen er oppfylt.

Førstvoterende fastslår, med henvisning til forarbeidene, at § 36 er en «*spesiell sitatregel som utvider medias rett til å gjengi visuelle verk*». Høyesterett ser det slik at denne utvidede retten kompenseres ved rettighetshaverens rett på vederlag for bruken. Bestemmelsen er dermed egnet til å «*balansere hensynene til informasjons- og ytringsfriheten – som er en bærebjelke i sitatretten – og rettighetshaverens legitime interesse i å få betalt for bruken.*» Høyesterett konkluderer med at når man er i området for regelen om dagshendinger i § 36 andre ledd, så er det denne avgrensningsregelen som må komme til anvendelse, og ikke den alminnelige sitatretten i § 29. Høyesterett presiserer likevel at det kan tenkes tilfeller der media kan ha adgang til å sitere visuelle verk etter § 29, f.eks. ved kortere utdrag fra filmverk eller der andres verk omtales i forbindelse med allmenn kunstkritikk, debatt, forskning eller som ledd i faglige vurderinger.

Det neste spørsmålet var om vilkårene for bruk etter § 36 andre ledd faktisk var oppfylt. Bestemmelsen angir:

«*Også et offentliggjort kunstverk, offentliggjort fotografisk verk eller offentliggjort filmverk som har tilknytning til dagshendingen uten å inngå i den, kan på samme vilkår som i første ledd gjengis mot vederlag. Dette gjelder ikke verk som er skapt i ervervsvirksomhet med henblikk på gjengivelse i media.*»

Høyesterett starter med en tolkning av vilkåret «*dagshending*». Førstvoterende forstår dagshendingsvilkåret slik at ikke bare nylig hendelser omfattes, og søker støtte for dette i EU-domstolens avgjørelser i sakene C-516/17 (Spiegel Online) og C-145/10 (Painer). Undersøkende journalistikk må også omfattes fordi krav om forhåndssamtykke ellers ville kunne begrense det journalistiske innholdet. Grensedragningen for hva som er en dagshending må videre bero på hvor sterkt hensynet til informasjons- og ytringsfriheten gjør seg gjeldende. I den foreliggende saken mente Høyesterett at man befant seg i kjernen av undersøkende journalistikk av stor allmenn interesse. Dagshendingsvilkåret var derfor «*klart*» oppfylt.

Gjengivelsen gikk heller ikke lenger enn «*formålet betinger*». Førstvoterende så en «*klar saklig sammenheng*» mellom fotografiene og teksten, og mente at fotografiene bidro til å belyse innholdet i saken.

Videre tok Høyesterett for seg om gjengivelsen av fotografiene var i tråd med «*god skikk*». Høyesterett fant her at det kunne gjøres visse innvendinger noen av endringene som var foretatt og mot mangelfulle kildehenvisninger. Sett opp mot sakens store allmenne interesse fant Høyesterett likevel at vilkåret var oppfylt.

Til sist vurderte Høyesterett om et krav om betaling av vederlag ville være i strid med EMK artikkel 10, noe Høyesterett kortfattet avviste.

Resultatet ble at fotografiene kunne brukes uten forhåndssamtykke, men det forutsetter betaling av vederlag, jf. åvl § 36 andre ledd. Saken går nå tilbake til lagmannsretten for utmåling av vederlaget.

Du kan lese saken med saksnummer HR-2022-1113-A i Lovdatas database *her*.

Skrevet av senioradvokat Hedda Baumann Heier og advokatfullmektig Emile Schønsby-Nolet ved Teknologi- og Medieavdeling i Oslo hos Advokatfirmaet Simonsen Vogt Wiig AS.

Gorrissen Federspiel

Tue Goldschmieding

Nye retningslinjer for prismarkedsføring

Den danske Forbrugerombudsmand offentliggjorde den 24. maj 2022 reviderede retningslinjer for prismarkedsføring. De nye retningslinjer træder i kraft den 28. maj 2022 samtidig med en ny bestemmelse i bekendtgørelse nr. 2292 af 12. marts 2021 (»den danske prismærkningsbekendtgørelse«) § 9 a, som ligger til grund for revideringen af retningslinjerne for prismarkedsføring.

De nye retningslinjer indebærer i det væsentligste, at normalprisperioden ændres til 30 dage mod tidligere 6 uger, og at tilbudsperioden ændres til 10 dage mod tidligere 14 dage. Derudover vil det ikke længere være muligt at undtage kortvarige kampagner af op til 3 dages varighed fra normalprisperioden på de 30 dage, idet normalprisperioden nu vil blive afbrudt af den kortvarige kampagne.

Ændringerne indebærer derudover, at varens normalpris skal angives ved alle meddelelser om prisnedsættelser. Endvidere indføres særlige regler for varer, som antages at blive forringet eller forældet hurtigt, idet disse varer skal have haft sin normalpris i mindst 14 dage, før et tilbud kan sammenlignes med denne pris. Varen kan herefter markedsføres med en nedsat pris i 5 dage. De tidligere særlige regler for dagligvarer og sæsonvarer ophæves, hvortil ovennævnte retningslinjer gælder i stedet.

Endelig medfører de nye retningslinjer, at det nu fremgår tydeligt heraf, at et produkt ikke må betegnes som »gratis«, hvis der som modydelse »betales« med data, hvis ikke den erhvervsdrivende har oplyst tydeligt herom.

Læs retningslinjerne her: https://www.forbrugerombudsmanden.dk/media/56754/forbrugerombudsmandens-retningslinjer-for-prismarkedsfoering.pdf

Læs Forbrugerombudsmandens pressemeddelelse her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2022/nye-retningslinjer-for-prismarkedsfoering/

Markedsføringsloven suppleres med nye regler for brugeranmeldelser

Den 28. maj 2022 trådte nye regler for brugeranmeldelser i kraft, eftersom bestemmelsen i lov nr. 2192 af 30. november 2021 (»den danske markedsføringslov«) § 6 b blev indført.

Bestemmelsen i markedsføringslovens § 6 b er baseret på artikel 7, stk. 6, i direktiv 2005/29/EF af 11. maj 2005 om urimelig handelspraksis, og medfører, at der stilles større krav til gennemsigtigheden af erhvervsdrivendes brug af brugeranmeldelser som led i deres markedsføring.

Hidtil har der ikke efter markedsføringsloven eksisteret specifikke regler for brugeranmeldelser, da disse var reguleret af det generelle forbud mod vildledende markedsføring, herunder forbuddet mod skjult reklame. Herudover anvendtes den danske Forbrugerombudsmands retningslinjer om offentliggørelse af brugeranmeldelser, som dog blot gælder brugeranmeldelser på egentlige anmeldelsesplatforme, heriblandt Trustpilot og lignende.

Den nye bestemmelse medfører, at erhvervsdrivende, der giver adgang til brugeranmeldelser af produkter, på en klar og forståelig måde skal oplyse, hvorvidt og i givet fald, hvordan den erhvervsdrivende sikrer, at de offentliggjorte anmeldelser stammer fra forbrugere, der faktisk har anvendt eller købt produkterne. Denne forpligtelse påhviler såvel erhvervsdrivende med en brugeranmeldelsesfunktion på deres egen hjemmeside som erhvervsdrivende, der giver adgang til brugeranmeldelser, som er foretaget gennem en tredjepart.

Supplerende udvides markedsføringslovens såkaldte sortliste med to nye bestemmelser med nr. 23 b og 23 c. De nye bestemmelser på sortlisten vedrører ligeledes brugeranmeldelser, og de medfører henholdsvis et krav til erhvervsdrivende om at træffe rimelige og forholdsmæssige foranstaltninger for at sikre, at en anmeldelse reelt stammer fra en forbruger, som har anvendt eller købt produktet, samt et forbud mod forkert fremstilling af brugeranmeldelser eller sociale anprisninger for at fremme produkter.

Læs ændringsloven her: https://www.retsinformation.dk/eli/lta/2021/2192

Læs bemærkningerne til lovforslaget her: https://www.retsinformation.dk/eli/ft/202112L00013

Lagring af indhold via cloud computing-tjenester er omfattet af undtagelsen om privatkopiering i direktiv 2001/29 artikel 5, stk. 2, litra b

Den 24. marts 2022 afsagde EU-Domstolen dom i sag

C-433/29 mellem Austro-Mechana Gesellschaft zur Wahrnehmung mechanisch-musikalischer Urheberrechte Geselsschaft mbH (»Austro-Mechana«) og Strato AG (»Strato«). Sagen var anlagt af den øverste regionale domstol i Wien, Østrig, som et præjudicielt spørgsmål angående en fortolkning af artikel 5, stk. 2, litra b, i direktiv 2001/29/EF af 22. maj 2001 om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet.

Austro-Mechana er et kollektivt ophavsretsforvaltningsselskab, som bl.a. varetager lovbestemte krav på vederlag. Den østrigske Urheberrechtsgesetz (ophavsretslov) af 9. april 1936, der finder anvendelse i nærværende sag, hjemler i sin § 42 b et krav på rimeligt vederlag (»lagringsmedievederlag«) for ophavsmanden under en række nærmere omstændigheder. Værket kan bl.a. være optaget på et i kommercielt øjemed fremstillet lagringsmedium, der efter dets karakter må påregnes at blive reproduceret ved optagelse på et lagringsmedium til egen eller privat brug, der herefter markedsføres i indlandet i kommercielt øjemed. Austro-Mechana påstod for Handelsgericht Wien (handelsretten i Wien, Østrig), at Strato skulle betale vederlag for »lagringsmedier af enhver art«, eftersom Strato leverer en tjeneste under navnet »HiDrive« til privat- og erhvervskunder, som stiller lagringsplads til rådighed for kunderne via en cloud computing-tjeneste.

I appelsagen ved Oberlandesgericht Wien (den øverste regionale domstol i Wien), forelagde den regionale domstol to spørgsmål for EU-Domstolen. Det første spørgsmål var, om udtrykket »reproduktioner på ethvert medium« i artikel 5, stk. 2, litra b, i direktiv 2001/29, skal fortolkes således, at bestemmelsen omfatter fremstillingen til privat brug af sikkerhedskopier af ophavsretligt beskyttede værker på en server, hvorpå udbyderen af en cloud computing-tjeneste stiller lagringsplads til rådighed for en bruger.

Domstolen konstaterede, at begrebet »reproduktion« skal fortolkes bredt og nåede frem til, at fremstillingen af en sikkerhedskopi af et værk på en lagringsplads, der stilles til rådighed for en bruger via en cloud computing-tjeneste, udgør reproduktion af værket som omhandlet i artikel 5, stk. 2, litra b, i direktiv 2001/29. Domstolen fortolkede dernæst »ethvert medium« som omhandlet i artikel 5, stk. 2, litra b, i bred forstand til også at omfatte servere som dem, der anvendes i forbindelse med cloud computing-tjenester. Domstolen nåede herefter frem til, at begrebet »ethvert medium« omfatter en server, hvorpå en udbyder af en cloud computing-tjeneste stiller lagringsplads til rådighed for en bruger.

Det andet spørgsmål, som Domstolen tog stilling til, var om artikel 5, stk. 2, litra b, i direktiv 2001/29 skal fortolkes således, at bestemmelsen er til hinder for en national lovgivning, hvorved den i bestemmelsen omhandlede undtagelse er gennemført, og som ikke pålægger udbydere af lagringsplads via cloud computing-tjenester at betale en rimelig kompensation for, at de fysiske personer, der gør brug af disse tjenester, uden tilladelse foretager sikkerhedskopier af ophavsretligt beskyttede værker til privat brug og til formål, der hverken direkte eller indirekte er kommercielle.

Domstolen nåede i den forbindelse frem til, at artikel 5, stk. 2, litra b, i direktiv 2001/29 ikke er til hinder for en sådan national lovgivning, forudsat at lovgivningen i øvrigt indeholder bestemmelser om betaling af en rimelig kompensation til rettighedshaverne. Således står det medlemsstaterne frit med henblik på finansieringen af den rimelige kompensation at indføre en afgift for privatkopiering ikke blot for de pågældende privatpersoner, men også for personer, der råder over udstyr, apparater og medier til digital reproduktion, og som i den forbindelse retligt eller faktisk giver privatpersoner adgang til dette udstyr eller tilbyder disse personer reproduktionstjenester. De betalingspligtige kan herefter lade afgiftsbeløbet for privatkopiering indgå i prisen for adgangen til udstyret, apparaterne, reproduktionsmedier m.v. og dermed overvælte den på privatbrugeren.

Læs hele dommen her: https://curia.europa.eu/juris/document/document.jsf?text=&docid=256462&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=5730658

Hvad skal der til for, at tredjemand har en »ældre rettighed« til et varemærke efter det gamle varemærkedirektivs artikel 6, stk. 2

Den 2. juni 2022 afsagde EU-Domstolen dom i sag C-112/21 mellem X BV og Classic Coach Company vof, herunder to fysiske personer, »A« og »B«. Sagen var anlagt af den Nederlandske øverste domstol, Hoge Raad der Nederlanden, som et præjudicielt spørgsmål angående fortolkning af reglerne i Europa-Parlamenters og Rådets direktiv 2008/95 EF af 22. oktober 2008) om varemærker (»varemærkedirektivet«).

Det fremgik af sagen, at X BV påstod, at Classic Coach samt »A« og »B« havde krænket dennes varemærkerettighed. Én af to brødre (»broder 1«) stiftede i 1975 selskabet BV X, som gjorde brug af to handelsnavne, hvoraf det ene svarede til brødrenes efternavn. BV X fik den 15. januar 2008 registeret et Benelux-ordmærke af handelsnavnet. Den anden broder (»broder 2«) havde videreført et selskab fra 1968 og havde i løbet af 1991 stiftet et interessentskab, som anvendte angivelser, svarende til navnet på broder 2 på turistbusserne. I løbet af 1995 forsatte broder 2's sønner »A« og »B« virksomhedens aktiviteter, som

med henblik herpå stiftede Classic Coach. Turistbusserne fra Classic Coach havde haft en angivelse, der indeholdt navnet på broder 2. BV X anså dette for en krænkelse af deres Benelux-ordmærke.

Den tyske appeldomstol, Gerechtshof Den Haag, fastslog at BV X havde en ældre ret til handelsnavnet end sagsøgte, men som følge af passivitet ikke kunne forbyde sagsøgtes anvendelse heraf. Det præjudicielle spørgsmål for Domstolen var, om det var et krav for at kunne fastslå en ældre rettighed, at indehaveren af denne rettighed kunne modsætte sig, at det yngre varemærke blev benyttet af indehaveren af dette. Yderligere blev der spurgt, hvorvidt en ældre rettighed kunne anerkendes for en tredjemand i en situation, hvor indehaveren af et yngre varemærke havde en ved den pågældende medlemsstats lovgivning anerkendt endnu ældre rettighed, registreret som varemærke.

Domstolen fortolkede artikel 6, stk. 2 i varemærkedirektivet således, at det ikke var et krav for at fastslå eksistensen af en ældre rettighed, at indehaveren af denne rettighed kunne modsætte sig, at det yngre varemærke blev anvendt af dennes indehaver. Domstolen lagde vægt på, at EU-lovgiver ikke ønskede at begrænse anvendelsesområdet for artikel 6, stk. 2, henset til, at en sådan betingelse ville fratage bestemmelsen enhver effektiv virkning. For at opfylde betingelserne i art. 6, stk. 2 er det således tilstrækkeligt, at den ældre rettighed med lokalt afgrænset karakter, er anerkendt i lovgivningen i den pågældende medlemsstat og anvendes erhvervsmæssigt.

I forhold til det andet spørgsmål, blev dette af Domstolen besvaret bekræftende, dersom indehaveren af varemærket og den endnu ældre rettighed ikke på grundlag af sin endnu ældre rettighed kunne forbyde tredjemands brug af sin yngre rettighed.

Læs hele dommen her: https://curia.europa.eu/juris/document/document.jsf?text=&docid=260186&pageIndex=0&doclang=DA&mode=req&dir=&occ=first&part=1&cid=4851510

Alka frifundet for at vildlede forbrugerne i reklamer for bilforsikringer

Østre Landsret har frifundet Alka Forsikring for at have vildledt forbrugere i reklamer om bilforsikringer på både TV og Alkas YouTube-kanal. Dette skete efter, at byretten i marts 2021 idømte Alka en bøde på 16,9 mio. kr. for at have overtrådt lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslovs«) forbud mod vildledning.

Det fremgik af sagen, at Alka i 2016 og 2017 har markedsført bilforsikringer som prisfaste, hvis bilen fik en skade. Dette blev markedsført uagtet, at der i forsikringsbetingelserne fremgik, at prisen og dækning kunne ændres med 14 dages varsel efter enhver anmeldt skade. Endvidere fremgik det af betingelserne, at i tilfælde af anmeldt skade, ville forbrugere få udsat en årlig præmienedsættelse og forhøjet deres selvrisiko med 4.000 kr. i det efterfølgende år.

Landsretten lagde i deres afgørelse vægt på, at Alka, uanset deres forsikringsbetingelser, ikke havde gennemført en prisstigning over for en kunde som følge af skade i gerningsperioden.

Landsretten fastlagde, at der ved vurderingen af, om en erhvervsdrivende har afgivet urigtige eller vildledende oplysninger, skal lægges vægt på både de formelle aftalevilkår, men også produktets reelle egenskaber. Den danske Forbrugerombudsmand mener, at et forsikringsprodukts egenskaber er fastlagt i aftalevilkårene og markedsføringen skal derfor stemme overens med vilkårene i denne. Forbrugerombudsmanden vil derfor drøfte spørgsmålet om indbringelse for Højesteret med Rigsadvokaten.

Læs Forbrugerombudsmandens pressemeddelelse her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2022/landsretten-frifinder-alka-for-vildledende-markedsfoering/

Sø- og Handelsretten: Novartis havde ikke retlig interesse i at få nedlagt forbud og påbud på baggrund at et patent, som endnu ikke var udstedt ved sagens anlæggelse

Sø- og Handelsretten afsagde den 17. juni 2022 dom i sagen BS-12527/2022-SHR mellem Novartis AG, Novartis Pharma AG, NOVARTIS HEALTHCARE A/S, Zentiva Denmark ApS (benævnes samlet »sagsøgerne«) og Viatris ApS.

Sagen udsprang af spørgsmålet om, hvorvidt de sagsøgte ville krænke sagsøgernes rettigheder i henhold til et europæisk patent, som endnu ikke var udstedt eller valideret, ved at udbyde, bringe i omsætning, markedsføre og anvende de generiske lægemidler Fingolimod »Glenmark«, Fingolimod »Mylan« og Fingolimod »Zentiva« i Danmark.

Sø- og Handelsretten fremhævede, at det som udgangspunkt er en betingelse for sagsanlæg, at sagsøger har retlig interesse i at få afgjort det spørgsmål, som den anlagte retssag vedrører. Heri ligger ligeledes, at der et krav om, at sagsøgers påstand har den fornødne aktualitet. Eftersom der ikke på tidspunktet for retssagen var udstedt et patent baseret på sagsøgers patentansøgning, fandt Sø- og Handelsretten, at sagsøger endnu ikke havde en ret til patentet, som kunne søges beskyttes i medfør af retsplejelovens § 413.

Sagerne er en principielle, eftersom de er de første af sine slags. Sagerne er kæret til Østre Landsret.

Læs hele kendelsen her: https://domstol.fe1.tangora.com/media/-300011/files/BS-12527-2022-SHR_m.fl._Kendelse.pdf

Sonion vinder over Huawei og Sony i patentsag ved Sø- og Handelsretten

Sø- og Handelsretten afsagde den 21. juni 2022, dom i sag BS-24619/2021-SHR mellem Sonion A/S og Sonion Nederland B.V. mod Huawei Technologies (Denmark) ApS, Huawei Technologies Sweden AB (herefter Huawei) og Power A/S. Samtidig blev der afsagt dom i sag BS-32103/2021-SHR mellem Sonion A/S og Sonion Nederland B.V. mod Sony Nordic Denmark.

Sagen udsprang af spørgsmålet om, hvorvidt de sagsøgte krænkede sagsøgerens patent- og brugsrettigheder på en »Voice Pick Up Bone Sensor«, der indgik i en række høretelefoner der blev markedsført af Sony og Huawei. Sensoren er en teknologi, udviklet af Sonion, der forstærker vibrationer i kæbebenet og kan derfor bruges til at identificere og isolere en stemme. Dette muliggør, at man kan gennemføre telefonsamtaler, hvor stemmen isoleres fra omgivelsernes støj. Produktet med sensoren blev solgt til en underleverandør til Huawei, der senere stoppede salget og Huawei udkom med sit eget headset med en »Voice Pick Up Bone Sensor«, der kunne det samme som den teknologi, som Sonion havde fået patent på. Sensoren var udviklet af selvsamme underleverandør, som Sonion havde solgt til. Senere blev Sony trukket ind i sagen, fordi Sonion sendte et headset på markedet med den samme sensor som den udarbejdet af Huaweis underleverandør.

Sø- og Handelsretten gav Sonion medhold i, at der forelå en krænkelse af Sonions rettigheder og der kunne nedlægges forbud mod Huawei og Sonys markedsføring af de krænkende produkter. Uanset, at Sony og Huawei gjorde gældende, at Sonions rettigheder manglede basis, nyhed og opfindelses- eller frembringelseshøjde, fandt Sø- og Handelsretten ikke, at Sony og Huawei havde godtgjort, at Sonions rettigheder var ugyldige.

Læs kendelsen i sagen mod Huawei og Power: https://domstol.fe1.tangora.com/media/-300011/files/BS-24619-2021-SHR_-_Kendelse.pdf?rev1

Læs kendelsen i sagen mod Sony: https://domstol.fe1.tangora.com/media/-300011/files/BS-32103-2021-SHR_-_Kendelse.pdf?rev1

Tue Goldschmieding, Gorrissen Federspiel

Oplysninger om, hvem der var leverandør til en webshop med negleprodukter var ikke en forretningshemmelighed

Sø- og handelsretten afsagde den 11. april 2022 dom i sagen BS-17442/2021-SHR mellem Codefort Projects ApS (»Codefort Projects«) og henholdsvis »A« og Brand Partners A/S (»Brand Partners«).

Sagen angik primært, hvorvidt »A« og Brand Partners havde overtrådt lov nr. 309 af 25. april 2018 (»den danske lov om forretningshemmeligheder«), ved at udnytte »A's« information om Codefort Projects' leverandør af negleprodukter, tilegnet som led i sin ansættelse hos sidstnævnte. Herudover angik tvisten, hvorvidt »A« og Brand Partners havde ageret i strid med god markedsføringsskik, jf. lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«), ved at fremtoning og indhold af deres webbutik til salg af negleprodukter, var påstået identisk med Codefort Projects'.

For så vidt angår bruddet på lov om forretningshemmeligheder fandt retten, at de kumulative betingelser efter legaldefinitionen i § 2 ikke var opfyldt, hvorfor der ikke var tale om udnyttelse af en forretningshemmelighed. Retten lagde vægt på, at oplysningerne om Codefort Projects' leverandør som en generel leverandør af negleprodukter var umiddelbart tilgængelig for aktører på markedet for salg af negleprodukter, bl.a. ved en almindelig søgning på e-handelsplatformen »Alibaba«. Hertil fremhævede retten, at Codefort Projects ikke havde foretaget de rimelige foranstaltninger til hemmeligholdelse af oplysningerne, såfremt der var tale om en hemmelig oplysning.

Derudover blev det ikke anset for godtgjort, at »A« ikke var kommet i besiddelse af informationen andetsteds fra, herunder ved almindeligt branchekendskab, og at »A« og Brand Partners havde anvendt en sådan fortrolig oplysning fra ansættelsen hos Codefort Projects til at etablere kontakt med leverandøren. Det blev i den forbindelse bemærket, at det ikke almindeligt er i strid med lov om forretningshemmeligheder, at man ved ansættelse opnår og udnytter almindelig branchekendskab.

I relation til den nedlagte påstand om overtrædelse af god markedsføringsskik, bemærkede retten at den af såvel Brand Partners som Codefort Projects' anvendte udformning af deres respektive fremtoning og indhold af deres hjemmesider, var foretaget på baggrund af generisk udbudte standardfunktioner gennem platformen Shopify. På baggrund heraf fandt retten ikke, at der var tale om et så tilstrækkeligt særpræg af Codefort Projects' stilmæssige fremtoning af webbutik og produkter, at disse burde nyde beskyttelse efter markedsføringsloven.

Som følge heraf, frifandt retten »A« og Brand Partners for overtrædelse af såvel lov om forretningshemmeligheder som brud på god markedsføringsskik efter markedsføringsloven.

Læs resumé her: https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-17442-2021-SHR.2372.aspx

Læs hele dommen her: https://domstol.fe1.tangora.com/media/-300011/files/BS-17442-2021-SHR_-_Dom_til_offentligg%C3%B8relse.pdf

Forbud og påbud vedrørende domænenavne, som krænkede Sketchers U.S.A.'s varemærke- og ophavsrettigheder

Sø- og Handelsretten afsagde den 2. juni 2022 kendelse i sagen BS-

6088/2022-SHR mellem Skechers U.S.A., Inc. II (benævnes »Skechers«) som sagsøger og Hi3G Denmark, Telia Danmark, Filial af Telia Nättjänester Norden, AB Sverige, Telenor A/S og Nuuday A/S som sagsøgte (benævnes samlet »sagsøgte«).

Sagen omhandlede, hvorvidt sagsøgte var forpligtet til at blokere for adgangen til domæner, hvor der pågik krænkelser af Skechers varemærke- og ophavsrettigheder. Endvidere var spørgsmålet, hvorvidt de sagsøgte fremadrettet var forpligtet til at blokere for adgangen til krænkede hjemmesider, dersom Skechers gjorde sagsøgte opmærksom herpå.

Hvad angik det første spørgsmål fandt Sø og Handelsretten, at sagsøgte ved at give deres kunder adgang til de af Skechers' nævnte hjemmesider, medvirkede til en krænkelse af Skechers' varemærkerettigheder og ophavsrettigheder. Betingelserne for at nedlægge forbud henholdsvis påbud som begæret efter lov nr. 1835 af 15. september 2021 (»den danske retsplejelov«) § 413, nr. 1, 2 og 3, og § 414, stk. 1, var derfor opfyldt.

For så vidt angik det andet spørgsmål fandt Sø- og Handelsretten, at påstanden ikke angik nogen bestemt hjemmeside eller nogen bestemt tredjepart, og følgelig ikke havde den fornødne klarhed og præcision. Hertil lagde Sø- og Handelsretten vægt på, at forbuds- og påbudsreglerne har til formål at indrømme en mulighed for, at Skechers hurtigere og gennem en almindelig retssag kan opnå et judicielt forbud eller påbud. Forbudsinstituttets særlige formål er netop, at give rettighedshavere en hurtig hjælp mod aktuelle eller truende retskrænkelser, hvorimod fremtidige, og ikke på nuværende tidspunkt aktuelle forhold, ikke er egnede til at blive behandlet i en mere sporadisk proces, som reglerne om foreløbige retsmidler medfører.

Læs resumé her: https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-6088-2022-SHR.2374.aspx

Læs hele kendelsen her: https://domstol.fe1.tangora.com/media/-300011/files/BS-6088-2022-SHR_Kendelse.pdf

Go Strøm politianmeldt for tredje gang for uønsket telefonsalg og vildledning

Den danske Forbrugerombudsmand oplyste i en pressemeddelelse af 24. marts 2021, at Forbrugerombudsmanden på ny har politianmeldt elselskabet Go Strøm for uønsket telefonsalg og vildledning af forbrugere.

Den tredje politianmeldelse af elselskabet skyldes opkald i perioden fra juli 2021 til februar 2022 til 75 forbrugere uden indhentelse af forudgående samtykke fra forbrugerne. Derudover har Go Strøm under disse telefonsamtaler vildledt 66 af forbrugerne ved bl.a. at udgive sig for at være forbrugerens nuværende elselskab, give forbrugerne urigtige oplysninger om pengebeløb til gode for eksempelvis en grøn elafgift samt tilmelde forbrugerne en el-aftale hos selskabet uden forbrugernes viden.

De eventuelt indgåede aftaler, som er indgået under telefonsamtalerne, vil være ugyldige, såfremt forbrugerne ikke har givet samtykke til telefonopkaldene fra Go Strøm. På samme måde vil aftalerne, som Go Strøm har vildledt forbrugerne til at indgå, være ugyldige.

Læs hele pressemeddelelsen her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2022/go-stroem-er-paa-ny-politianmeldt-for-ulovligt-telefonsalg/

Forbrugerombudsmanden anlægger retssag mod Tryg Forsikring A/S for at hæve forsikringspriserne uden at varsle prisstigningerne først

I en pressemeddelelse af den 13. april 2022 meddelte den danske Forbrugerombudsmand, at have indledt en retssag mod Tryg Forsikring A/S (»Tryg«).

Det fremgår af sagen, at Tryg over en periode på 4 år havde hævet priserne på privatkunders forsikringer uden at varsle om prisstigningerne.

Tryg's forsikringsbetingelser har følgende ordlyd »*Vi varsler væsentlige ændringer af betingelser og/eller prisen senest 30 dage før forsikringsperioden den udløber*«. Forbrugerombudsmanden mente således, at Tryg ikke havde hjemmel til at hæve priserne uden forinden at orientere kunderne derom. Prisstigningerne vedrørte følgende forsikringstyper: Indbo, ulykke, rejse, hus, bil, båd, hund, kat, knallert og motorcykel.

Forbrugerombudsmanden mente derudover, at en forsikringsaftale, hvor prisstigninger ikke ville blive varslet til kunderne, ville være ugyldig. En sådan aftale ville ifølge Forbrugerombudsmanden stride mod reglerne om hæderlig forretningsskik og urimelige aftalevilkår.

Hvis forbrugerombudsmanden får medhold i sagen, vil mange af Tryg's kunder kunne kræve prisstigningerne tilbagebetalt.

Læs hele pressemeddelelsen her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2022/forbrugerombudsmanden-staevner-tryg-forsikring/

Tue Goldschmieding er partner i Gorrissen Federspiel og en av de danske redaktørene for Lov&Data.


Gunnar Hjalt, Joel Tholin,
Nathalie Lindes Sjölander, Leonard Garg

Vägledande avgörande angående intrång i europeiskt patent som inte ännu meddelats, PMÖ 5185-22

Kärandens talan avsåg vid Patent- och marknadsdomstolen (PMD) fullgörelsetalan (vitesförbud, förstörelse m.m.) och en fastställelsetalan om ersättningsskyldighet grundat på patentintrång.

PMD avvisade kärandens talan i dess helhet på grund av att något patent ännu inte var meddelat.

Käranden överklagade till Patent- och marknadsöverdomstolen (PMÖD) som meddelade prövningstillstånd. Frågan som PMÖD hade att ta ställning till var om det fanns förutsättningar att avvisa kärandens talan innan stämning utfärdades på grund av att ett patent ännu inte var meddelat.

PMÖD framhöll att en allmän regel inte kan ställas upp för att avgöra frågan om talan kan väckas i situationer när en immateriell rättighets uppkomst är sannolik eller nära förestående. En bedömning måste göras i varje enskilt fall. Enligt tidigare praxis kan en sådan talan avvisas när det inte finns förutsättningar att påbörja en meningsfull förberedelse av målet.

I det aktuella målet hade käranden fått ett skriftligt beslut från Europeiska patentverkets besvärskammare att patent skulle meddelas, med förväntad expediering av beslutet i slutet av juni 2022. Patentet bedömdes alltså kunna meddelas i augusti 2022, men det ansågs inte vara sannolikt att målet i Patent- och marknadsdomstolen skulle kunna avgöras slutligt före augusti 2022.

PMÖD fann inte att det inte fanns något hinder mot att väcka den aktuella talan.

Det överklagade beslutet undanröjdes därför och målet återförvisades till PMD för fortsatt behandling.

Se avgörandet i dess helhet här: https://www.domstol.se/patent--och-marknadsoverdomstolen/patent--och-marknadsoverdomstolens-avgoranden/2022/114149/

Begäran om förhandsavgörande avseende Bryssel I-förordningen vid mål om patentintrång, PMÖ 671-21

Innehavaren av ett europeiskt patent, som hade validerats i Österrike, Tyskland, Spanien, Frankrike, Storbritannien, Grekland, Italien, Nederländerna, Sverige och Turkiet, väckte talan i Sverige mot ett svenskt företag med dotterbolag i flera andra europeiska länder. Innehavaren ville att det svenska företaget skulle förbjudas att nyttja den patenterade uppfinningen i de ovan nämnda länderna samt förpliktigas att utge ersättning för det olovliga nyttjandet. Det svenska företaget yrkade att domstolen skulle avvisa talan avseende alla länder utom Sverige eftersom domstolen inte var behörig att ta upp talan till prövning med anledning av artikel 24.4 i Europaparlamentets och rådets förordning (EU) nr 1215/2012 av den 12 december 2012 om domstols behörighet och om erkännande och verkställighet av domar på privaträttens område (Bryssel I).

Den i målet aktuella artikel 24.4 i Bryssel I-förordningen innebär ett undantag från huvudregeln om att talan ska väckas där svarandens har hemvist, artikel 4.1. , och anger att en talan, oavsett om det är ett käromål eller ett svaromål, som avser registrering eller giltighet av patent ska prövas i det land där patentet registrerats.

Begreppet ”intrång” nämns inte uttryckligen i artikeln men en fråga om intrång i patent kan ofta förekomma i mål om patents giltighet. Eftersom artikel 24.4. avser såväl svaromål som käromål kan det antas att 24.4. skulle kunna vara tillämpligt på en talan om intrång där en invändning om ogiltighet har gjorts, initialt eller i efterhand.

Patent- och marknadsdomstolen (PMD) avvisade innehavarens talan avseende de utländska patenten, med hänvisning till att artikel 24.4. anger att domstolar i andra stater har exklusiv behörighet att pröva giltigheten av de patent som har validerats där.

Innehavaren överklagade till PMÖD som identifierade att rättsläget var oklart på några punkter. Förutom frågan om intrångstalan omfattas av regleringen i artikel 24.4 ansåg PMÖD att det oklart om nationella regler om hur ogiltighet av patent ska prövas påverkar frågeställningen i artikel 24.4. samt till sist om Bryssel I-förordningen kunde utsträckas till Turkiet som inte är en unionsstat.

PMÖD vände sig till EU-domstolen och begärde ett förhandsavgörande, för besvarande av följande frågor:

1. Ska artikel 24.4 i Bryssel I tolkas så att ordalydelsen ”*talan, oavsett om det är fråga om ett käromål eller ett svaromål, som avser registrering*

eller giltighet av patent", innebär att en nationell domstol, som i enlighet med artikel 4.1 i Bryssel I konstaterat sig behörig att pröva en tvist om patentintrång, inte längre är behörig att pröva intrångsfrågan, om en invändning görs om att det ifrågavarande patentet är ogiltigt, eller ska bestämmelsen tolkas så att den nationella domstolen endast blir obehörig att pröva invändningen om ogiltighet?

2. Påverkas svaret i fråga 1 av om det i nationell rätt finns bestämmelser, motsvarande de som finns i 61 § andra stycket patentlagen, som innebär att en ogiltighetsinvändning som framställs i ett intrångsmål för att kunna prövas förutsätter att svarande väcker en separat talan om ogiltighet?
3. Ska artikel 24.4 i Bryssel I tolkas så att den gäller i förhållande till en domstol i ett tredjeland, dvs. i det aktuella fallet så att den även ger exklusiv behörighet för domstol i Turkiet för den del av det europeiska patentet som validerats där?

Se avgörandet i dess helhet: https://www.domstol.se/patent--och-marknadsoverdomstolen/patent--och-marknadsoverdomstolens-avgoranden/2022/114432/

Vissa frågor relaterade till nyttjande av upphovsskyddade rättigheter under konsultavtal, PMT 4780-21

I ett avgörande från Patent- och marknadsöverdomstolen (PMÖD) behandlades diverse frågor relaterade till nyttjanden av upphovsrättsligt skyddade fotografiska och litterära verk som hade skapats till följd av ett konsultuppdrag. Verken, som bestod av porträttbilder och intervjuer till en kommande utställning på ett museum, hade skapats av konsulten och uppdraget som sådant hade formaliserats i ett konsultavtal mellan konsulten och uppdragsgivaren (en stiftelse). Efter att bilderna och intervjuerna hade nyttjats av uppdragsgivaren på diverse sätt, däribland på utställningen, på uppdragsgivarens sociala medier och i en mobilapplikation, uppkom frågor bland annat om konsulten hade rätt till ytterligare ersättning för vissa av uppdragsgivarens förfoganden. Av vikt för frågorna var tolkningen av parternas avtal som bland annat innehåll en s k immaterialrättsklausul. Av immaterialrättsklausulen följde bland annat att rättigheterna skulle tillfalla konsulten, men att uppdragsgivaren gavs en icke-exklusiv och till tredje part upplåtbar rätt att förfoga över rättigheterna under vissa angivna förutsättningar, däribland i förhållande till uppdragsgivarens "alla egna medieformer". Vid en upplåtelse till tredje part angavs vidare att konsulten skulle vara berättigad till viss ytterligare ersättning. PMÖD prövade ifall det i något av fallen, däribland i förhållande till publiceringen via appen och på sociala medier, kunde anses ha visats att det förekommit en upplåtelse till tredje part som enligt avtalet skulle berättiga ytterligare ersättning, och fann att så inte var fallet. Käromålet ogillades av PMÖD, som i flertalet frågor ansåg att konsulten i många avseenden inte hade uppfyllt sin bevisbörda. Målet innehöll även till viss del några övriga frågor, bland annat tolkning av rättighetsupplåtelses giltighetstid, eventuella olovliga förfoganden samt bättre rätt till varumärke.

Se avgörandet i dess helhet här: https://www.domstol.se/patent--och-marknadsoverdomstolen/patent--och-marknadsoverdomstolens-avgoranden/2022/113653/

Gunnar Hjalt, Senior Counsel, Joel Tholin, Associate, Nathalie Lindes Sjölander, Trainee, Leonard Garg, Trainee, Bird & Bird Advokat.

SELMER

Vemund Sande

Kan force majeure påberopes ved cyberangrep?

Et cyberangrep kan få store konsekvenser for virksomheten som rammes. Ikke bare kan den rammede bli presset til å betale løsepenger for å få tilbake data eller lignende. Angrepet kan også medføre nedetid og tilhørende problemer med å oppfylle kontraktuelle forpliktelser overfor kunder eller andre. I denne artikkelen vil vi se nærmere på hvorvidt den som er rammet av et cyberangrep kan påberope seg at dette er en force majeure-situasjon som suspenderer de kontraktuelle pliktene under den rammedes avtaler.

De aller fleste avtaler mellom næringsdrivende inneholder en klausul som sier at dersom en såkalt force majeure-hendelse hindrer (eller vesentlig vanskeliggjør) en parts oppfyllelse av sine plikter under avtalen suspenderes disse pliktene så lenge situasjonen varer. Det er ordlyden i den konkrete avtalen som vil være utgangspunktet for vurderingen av om et cyberangrep oppfyller kravene til force majeure. Statens standardavtale om løpende tjenestekjøp over internett (SSA-L) inneholder følgende vilkår for å kunne påberope seg force majeure: «*Skulle det inntreffe en ekstraordinær situasjon, som gjør det umulig å oppfylle plikter etter denne avtalen, og som etter norsk rett må regnes som force majeure, skal motparten varsles om dette så raskt som mulig.*» Her er det flere ting å merke seg som er relevant for cyberangrep. Det må foreligge en ekstraordinær situasjon som umuliggjør oppfyllelse. Vanlige hendelser kvalifiserer ikke som force majeure. Det er videre oppstilt et strengt krav om innvirkning på muligheten for å oppfylle. Det innebærer et krav om årsakssammenheng mellom situasjonen (cyberangrepet) og oppfyllelsen. Etter bakgrunnsretten som SSA-L også viser til, vil det være nok dersom oppfyllelse vil være praktisk umulig. Det er derfor usikkert om SSA-L skal forstås slik at det kreves absolutt umulighet. Etter bakgrunnsretten inneholder force majeure-begrepet i tillegg til vilkårene om at det må være en ekstraordinær situasjon som gjør det (praktisk) umulig å oppfylle, også et krav om at situasjonen må ligge utenfor hva parten kunne tatt i betraktning på avtaletiden. Manglende forbehold utelukker også vanligvis at hindringen tillegges betydning, dersom slikt forbehold burde vært tatt. Vilkårene henger sammen, og vurderingene vil til en viss grad være overlappende.

Force majeure har historisk sett vært forbeholdt krig, streik, naturkatastrofer og andre lignende ekstraordinære hendelser. I lys av den teknologiske utviklingen er det imidlertid naturlig at også cyberangrep og -krigføring kan anses som slike ekstraordinære hendelser. Vilkåret om at en situasjon må være «ekstraordinær» for å kvalifisere som force majeure tilsier imidlertid at det må stilles krav til cyberangrepets art. Angrep av den typen virksomheter blir utsatt for på jevnlig basis kan ikke sies å være ekstraordinære. For at et cyberangrep skal anses som force majeure må det være av en art, form, størrelse og/eller lignede som ikke forventes. Denne vurderingen vil være overlappende med vurderingen av hvorvidt situasjonen lå utenfor hva partene burde tatt betraktning på avtaletidspunktet.

I en del force majeure-klausuler angis visse eksempler på slike ekstraordinære hendelser. I IT-kontrakter nevnes gjerne cyberangrep som ett av disse, og da er det ordlyden i avtalen som avgjør hvilke typer angrep som omfattes.

Videre stilles det som nevnt krav om at den manglende oppfyllelsen skyldes force majeure-situasjonen (årsakssammenheng). For en IT-leverandør gjelder dette for eksempel dersom angrepet lammer systemet som leveres, slik at kunden ikke kan benytte det som forutsatt i avtalen. Angrepet kan forekomme både hos leverandøren selv og hos kunden. Et eksempel på sistnevnte er det omfattende cyberangrepet i mars 2019 mot Hydro, som er en

stor innkjøper av IT-tjenester. I slike tilfeller kan det tenkes at både kunde og leverandør påberoper force majeure overfor sine respektive kunder dersom manglende oppfyllelse skyldes angrepet.

De vanlige vilkårene for å anerkjenne et cyberangrep som force majeure krever videre at adekvate forbehold/tiltak er satt i verk for å unngå angrepet eller overvinne følgene av angrepet. Det oppstilles dermed et krav om tilstrekkelig IT-sikkerhet. Slike krav er ofte uttrykkelig nedfelt i avtalen. I de tilfellene detaljerte krav foreligger i avtalen kan det virke logisk å se på dette som førende for hva som forventes, uten at de nødvendigvis må betraktes som uttømmende. Et naturlig spørsmål i forlengelsen av dette er om de kravene som stilles til IT-sikkerhet i forbindelse med behandling av personopplysninger under personvernforordningen (GDPR) oppfyller disse kravene. Dette er spesielt aktuelt for IT-kontrakter ettersom leveransen under disse avtalene ikke sjeldent innebærer behandling av personopplysninger.

Ettersom force majeure er ment å være et snevert unntak fra hovedregelen om at avtaler skal holdes, taler gode grunner for at virksomheter må ha informasjonssikkerhet som er blant den beste i bransjen, og som sikrer virksomheten mot forventede og påregnelige cyberangrep. Force majeure skal vurderes konkret for den enkelte avtalesituasjon, og det er lett å se for seg at domstolene vil stille særlig strenge krav til for eksempel en IT-leverandørs egen IT-sikkerhet eller til IT-sikkerhet for IT-systemer som er kritiske for en virksomhets drift og produksjon.

Så vidt vi vet har ikke domstolene enda behandlet hvilke krav som stilles til virksomheters IT-sikkerhet i forbindelse med force majeure. Det blir spennende å se hvilken terskel man vil legge seg på dersom en slik sak kommer opp.

Vemund Sande er fast advokat i avdelingen for HITEK i Advokatfirmaet Selmer, Oslo.

Gorrissen Federspiel

Tue Goldschmieding

Ny version af standardkontrakten for it-drift, D17, offentliggjort

Den 10. maj 2022 blev version 4 af standardkontrakten for it-drift, D17, offentliggjort.

Version 4 af D17 er den hidtil mest omfattende opdatering af standardkontrakten. Én af de væsentligste nyskabelser er, at D17 nu indeholder en regulering af ansvaret for public cloud-ydelser. Arbejdsgruppen bag D17 har fundet en afbalanceret model, hvor den danske driftsleverandør tager ansvaret for valget af cloud-leverancer samt også er pålagt en pligt til at rådgive kunderne om disse leverancer. Men når først driftsydelsen, inkl. cloud-leverancerne, er sat i drift, afgrænses den danske driftsleverandørs ansvar til et ansvar i henhold til vilkårene fra public cloud-leverandøren, dvs. et back-to-back-ansvar. Anvendelsesområdet for D17 og dens praktiske anvendelighed udvides dermed betydeligt.

Den nye version af D17 indeholder herudover en række andre opdateringer på væsentlige områder, eksempelvis (i) reguleringen af ansvar og opgaver omkring kundens tredjepartskontrakter, (ii) adressering af kravene til it-sikkerhed, (iii) tilgangen til håndteringen af overdragelsesplaner og ophørsbistand, (iv) introduktion og regulering af Kritiske Servicemål, (v) "fix and deliver first, settle later", og (vi) ansvarsregulering ved persondatakrænkelser.

Standardkontrakten, D17, er, med få undtagelser, udtryk for et agreed document, dvs. en standardkontrakt, der nyder opbakning fra både kunde- og leverandørorganisationer.

D17 opdateres løbende med angivelse af versionsnummer.

Læs D17-standardaftalen v. 4.0 her: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fd17.dk%2Fwp-content%2Fuploads%2F2022%2F02%2FD17-v4-FINAL.docx&wdOrigin=BROWSELINK

https://www.twobirds.com/da/insights/2022/denmark/ny-version-af-standardkontrakten-for-it-drift,-d17,-er-netop-blevet-offentliggjort

Ny version af standardkontrakten for it-drift, D17, på vej - Bird & Bird (twobirds.com)

Nyt katalog over kontraktbestemmelser skal sikre myndigheders styring med leverandører af samfundskritiske IT-systemer

Den danske Digitaliseringsstyrelse udgav den 4. marts 2022 et nyt katalog over kontraktbestemmelser for samfundskritiske it-systemer, som myndighederne skal implementere i nye kontrakter efter et følg-eller-forklar princip.

Kataloget er udarbejdet af en arbejdsgruppe bestående af det danske Justitsministerium, det danske Forsvarsministerium, den danske Udvikling- og Forenklingsstyrelse og Digitaliseringsstyrelsen. Desuden har Optimum IT og Kammeradvokaten bistået i forløbet. Kataloget udspringer af initiativ 3.3 i den Nationale Strategi for Cyber- og Informationssikkerhed 2018-2021, som overordnet har til formål at få bedre styr på leverandører af samfundskritiske it-systemer. Kataloget søger at øge informations- og forsyningssikkerheden for myndighedernes samfundskritiske it-systemer.

Kataloget har fire kontrakttemaer for øje, nemlig driftsafvikling, sikkerhed, persondata og kontrol. Myndighederne får igennem benyttelsen af kontraktbestemmelserne nogle styringsredskaber. Som konkret eksempel kan nævnes step-in-rettigheder og ejerskiftekontrol. Bestemmelserne kan operationaliseres gennem K04, standardkontrakten for it-drift samt det appendiks som offentliggøres sammen med kataloget. Den foreslåede operationalisering behøver dog ikke følges af myndighederne, der i stedet kan vælge at anvende egne kontraktskabeloner, såfremt de indarbejder katalogets bestemmelser.

Følg-eller-forklar princippet medfører, at myndighederne skal implementere alle bestemmelserne i kataloget, medmindre myndigheden kan forklare, hvorfor en bestemmelse under hensyntagen til særlige forhold, ikke bør indgå i en specifik kontrakt.

Læs nyheden her: https://digst.dk/nyheder/nyhedsarkiv/2022/marts/katalog-samfundskritiske-it-systemer/

Læs hele kataloget her: https://sikkerdigital.dk/Media/637819816667401542/Katalog%20over%20kontraktbestemmelser_2022_web.pdf

Tue Goldschmieding er partner i Gorrissen Federspiel og en av de danske redaktørene for Lov&Data.

KLIMANØYTRAL DISTRIBUSJON
Levert av Posten

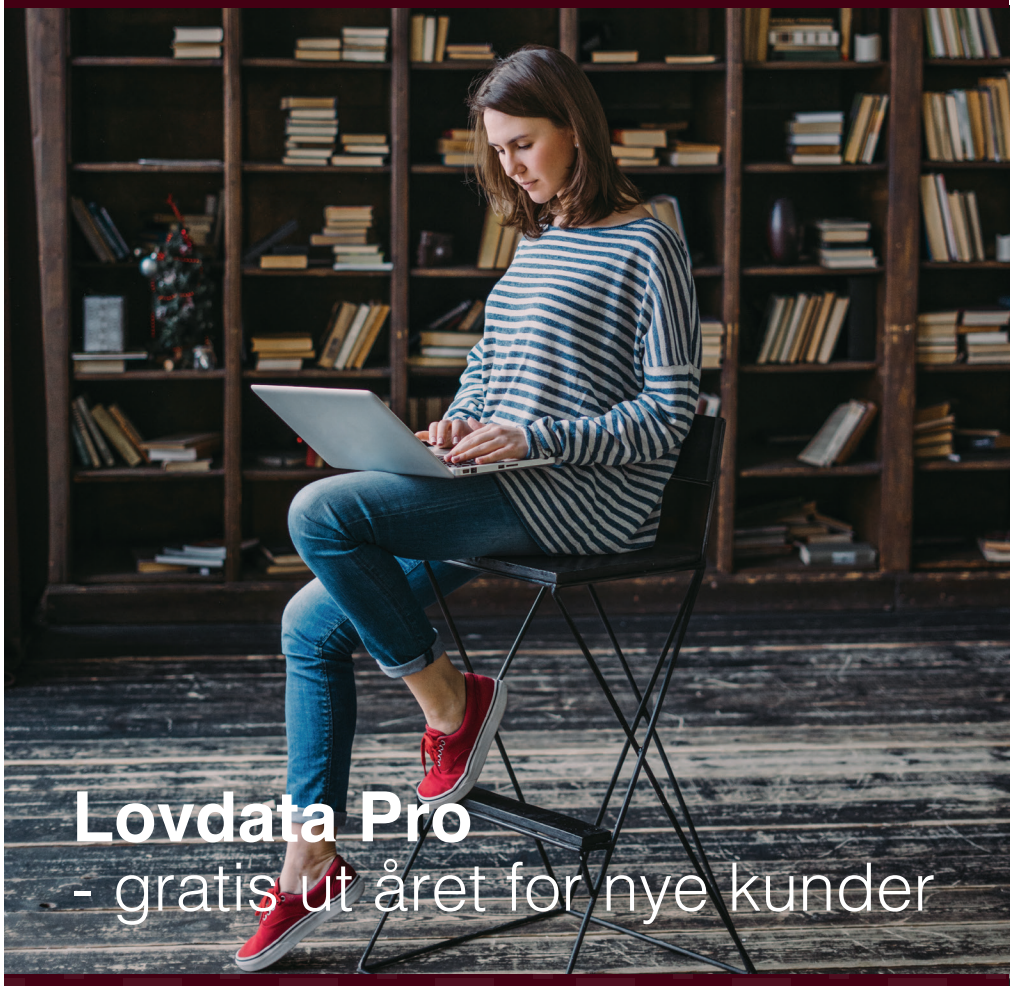
NORGE P. P.
posten

Returadresse:
Lovdata
Pb. 6688 St. Olavs plass
NO-0129 Oslo
Norge

Nytt fra

LOVDATA

LOVDATA
PRO



Lovdata Pro
- gratis ut året for nye kunder

pro.lovdata.no

Produksjon: 07 Media AS