Lov & Data

Nr. 133
Mars 2018

Nr. 1/2018

Innhold








Lov&Data

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

Lovdata
Postboks 2016 Vika
NO-0125 Oslo, Norge
Tlf.: +47 23 11 83 00
Faks: +47 23 11 83 01
E-post: lovogdata@lovdata.no
Nettside: www.lovdata.no

Lovdata forbeholder seg rett til å bruke artikler og domsreferater i Lovdatas elektroniske systemer.

Ansvarlig redaktør er Jarle Roar Sæbø, juridisk direktør i HPE, Oslo og leder for Domeneklagenemnda.
Medredaktør er Sandra Stenersen Henden, Lovdata.
Redaktører for Danmark er dr.juris Henrik Udsen ved Center for informations- og innovationsret, Københavns universitet og Tue Goldschmieding, partner i firmaet Gorrissen Federspiel, København.
Redaktør for Sverige er doktorand Daniel Westman, Institutet för rättsinformatik ved Stockholms universitet.
Fast spaltist er Halvor Manshaus, partner i advokatfirmaet Schjødt.

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

Abonnementspriser for 2018
Norge: nkr 370,- pr. år
Utland: nkr 450,- pr. år
Studenter, Norge: nkr 175,- pr år
Studenter, utland: nkr 235,- 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 og Svenska föreningen för IT och Juridik (ADBJ). 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/*

MILJØMERKET TRYKKERI 01 MEDIA – 2041 0379

Privacy by Design – Hvad kræves egentlig?

'Privacy by Design' er for alvor sat på tapetet med GDPR. Men det er ikke et nyt begreb, som er opfundet af Kommissionen. Begrebet er lige så gammelt som informationssamfundet selv og den deling af data, som samfundsudviklingen har medført. Det er en grundlæggende tanke om, at databeskyttelse ikke blot er overholdelse af den regulatoriske ramme, som GDPR opstiller, men i stedet må tænkes ind i en virksomheds it-infrastruktur som en integreret del heraf.

Mange virksomheder står nu med overvejelser om, hvordan dette begreb skal håndteres og implementeres, hvor mange ressourcer der skal investeres og hvad skal man som virksomhed gøre i forhold til den eksisterende it-infrastruktur? Der er ikke meget vejledning at finde for at træffe den rigtige beslutning.

Men som det også fremgår af GDPR art. 25, så er Privacy by Design et fleksibelt begreb. Den danske betænkning nr. 1565 i kommentarerne til art. 25, at persondata-direktivets art. 17, stk. 1 om tekniske og organisatoriske foranstaltninger og den danske sikkerhedsbekendtgørelse indeholder allerede nu lignende forpligtelser, som der kan findes støtte i for vurderingen. Ved vurderingen af hvilke konkrete tiltag for et givet system er nødvendige, er relevante momenter; behandlingens karakter, risici og sandsynlighed, samt alvoren af den fare, som behandlingen udgør for de registrerede. Disse understreger også begrebets sammenhæng med risikoanalysen i artikel 35. Dertil kommer, ikke mindst, at implementeringsomkostningerne også kan indgå som en legitim faktor.

For eksisterende it-systemer, har det danske Justitsministerium på stormøde den 13. juni 2017 tilkendegivet, at Privacy by Design må forstås som et fremadrettet krav, og eksisterende systemer skal derfor ikke gennemgå større renovationer for at understøtte Privacy by Design. Eksisterende systemer skal dog stadig overholde regler for behandling af persondata og tekniske og organisatoriske foranstaltninger må tages, som eksempelvis data minimering eller access restriction eller optimal udnyttelse af standardindstillinger. Ved udskiftning eller opgradering af it må databeskyttelse dog indgå på lige fod og i sammenhæng med sikkerhedsvurderingen af mulige løsninger.

På mange måder er gennemførelsen af Privacy by Design derfor i ligeså høj grad stilet til de systemudviklere, som skal kunne tilbyde denne løsning i fremtiden, både interne og eksterne udviklere. Systemudviklere bør derfor anerkende det marked, hvor netop deres løsninger kan møde et vedvarende behov på databeskyttelse. Og på samme måde må virksomhederne sætte Privacy by Design på listen over nødvendigheder ved både intern udvikling og køb af ekstern it.

Tue Goldschmieding

I kjølvannet av Schrems:

Internasjonal dataflyt og balkaniseringen av internett

av Eva Jarbekk og Anne-Marit Wang Sandvik, Schjødt.

Eva Jarbekk

Anne-Marit Wang Sandvik

Dataflyt over landegrensene er avgjørende for utallige multinasjonale selskaper. De fleste av oss bruker også tjenestene til amerikanske og asiatiske teknologiselskaper hver dag uten å tenke over hvor dataene våre faktisk er. Vi har også, uten bekymring, lagret personlige opplysninger i skyer over både Korea, India og USA. Nå truer flere søksmål og ulik nasjonal lovgivning i horisonten. 2018 kan vise seg å bli et skjebneår for den internasjonale utvekslingen av personopplysninger slik vi kjenner den.

Den nye personvernforordningen

EUs nye personvernforordning (GDPR) trer i kraft den 25. mai.[1] Forordningen er en milepæl for personvernet, og gir europeiske borgeres personopplysninger en høy grad av beskyttelse. GDPRs geografiske virkeområde gjør at ringvirkningene av forordningen kan merkes i hele verden. Alle selskaper som tilbyr tjenester til, eller behandler personopplysninger for europeere må følge forordningen. Noen selskaper har valgt å gjennomføre endringer for å etterleve loven, andre velger å ta sjansen på at GDPRs lange arm ikke skal rekke ut til det hjørnet av verden der deres serverpark og hovedkontor, så skatterettslig fordelaktig, er plassert. Tiden vil vise om dette er en bærekraftig strategi.

GDPR viderefører også den forholdsvis strenge reguleringen i nåværende personvernlovgivning for overføring av personopplysninger til såkalte tredjeland[2]. Det vil si land som ikke er ansett å behandle personopplysninger i henhold til europeiske standarder. Etter GDPR vil overføring til slike tredjeland være forbudt, med mindre det foreligger et særskilt rettslig grunnlag.[3] Gjeldende personvernlovgivning tilbyr et utvalg slike rettslige grunnlag, og disse vil også gjelde etter GDPR. De absolutt mest brukte grunnlagene er Privacy Shield for overføringer til USA og EUs standardavtaler for overføringer til USA, og resten av verden.[4] Begge grunnlag går en usikker tid i møte. For EUs standardavtaler (Standard Contractual Clauses - SCC) vil skjebnen sannsynligvis avgjøres av EU-domstolen i løpet av 2018. For Privacy Shield vil overlevelse blant annet avhenge av hvorvidt anbefalingene

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

2 Lov om behandling av personopplysninger (personopplysningsloven) av 14. april 2000 nr. 31 § 29 første ledd; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Artikkel 25

3 Regulation (EU) 2016/679 Kapittel V

4 Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC [2001] OJ L181/19; Commission Decision 2004/915/EC of 27 December 2004 amending decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries [2004] OJ L385/74; Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council

til Artikkel 29-gruppen blir innarbeidet før 25. mai.

Schrems og kampen mot EUs standardkontrakter

Max Schrems har blitt en kjent figur i de siste årene. Historien om hvordan han fikk ugyldiggjort Safe Harbour, er blitt en klassiker - i hvert fall i personvernkretser. Men Schrems er åpenbart ikke en som hviler på laurbærene. De siste to årene har han fortsatt sin kamp mot Facebook, og nok en gang står et rettslig grunnlag for overføring av personopplysninger til tredjeland på spill, og denne gangen kan avgjørelsen bli enda mer vidtrekkende.

I etterkant av Schrems' seier mot Safe Harbour gikk Facebook over til å bruke EUs standardkontrakt som grunnlag for å overføre personopplysninger til USA.[5] Schrems klaget deretter Facebooks bruk av SCCs inn for det irske datatilsynet og argumenterte for at SCCs strider mot EUs charter om grunnleggende rettigheter.[6] Det irske datatilsynet ble overbevist, men fastholdt at de ikke hadde jurisdiksjon til å ugyldiggjøre SCCs. De bestemte seg derfor for å ta saken videre til domstolen.

I retten argumenterte det irske datatilsynet for at SCCs, som grunnlag for overføring av personopplysninger til USA, må anses ugyldig fordi det strider mot artikkel 47 (rett til effektivt rettsmiddel) og artikkel 7 og 8 (retten til privatliv) i EUs charter om grunnleggende rettigheter.

SCCs utgjør en kontraktsforpliktelse som pålegger selskaper i tredjeland å behandle europeiske personopplysninger i henhold til europeiske personvernprinsipper. Datatilsynets argument var at SCCs ikke kan utgjøre en slik reell forpliktelse, all den tid amerikanske myndigheter har full tilgang til personopplysninger fra Facebook.

Saken ble behandlet i Irish High Court i 2017 og den 3. oktober 2017 kom dommen.[7] Høyesterettsdommer Costello var enig med det irske datatilsynet i at det var «valid grounds for concern» og at spørsmålet må behandles av EU-domstolen.

Det som bekymret det irske datatilsynet, og som den irske høyesterett var enig i, er hovedsakelig to ting. For det det første, at personopplysninger som overføres fra Europa til USA er lett tilgjengelig for amerikanske myndigheter og at SCCs dermed faktisk ikke kan beskytte opplysningene fra behandlingen til amerikanske myndigheter. For det andre; fordi SCCs ikke kan beskytte opplysningene fra amerikanske myndigheter kan de heller ikke tilby europeere et effektivt rettsmiddel for krenkelsen av deres personvern. De facto tilbyr dermed SCCs ingen av de tingene som klausulene er ment å gjøre. Bakgrunnen for disse bekymringene er blant annet paragraf 702 i den amerikanske Foreign Intelligence Surveillance Act (FISA).[8]

> "Personopplysninger som overføres fra Europa til USA er lett tilgjengelig for amerikanske myndigheter

Det såkalte 702-programmet gir amerikansk etterretning svært vide fullmakter til å hente inn personopplysninger gjennom såkalte bakdører hos de store teknologiselskapene, blant annet Facebook og Google. Myndighetene har, etter punkt 702, mulighet til å hente ut informasjon først, og spørre om lov etterpå. Det vil si at de får lese informasjonen før de ber retten om lov til å bruke den. Det innebærer naturlig nok at myndighetene får tilgang til og gjennomgår en stor mengde informasjon som ingen har oversikt over og som høyst sannsynlig ikke er relatert til straffbare handlinger.

702-programmet har vært heftig debattert og president Donald Trump har vært en ivrig forkjemper for programmet. Programmet, som består av en midlertidig tillegg til FISA, har vært gjeldende i 6 år og skulle etter planen utløpe i april 2018. 702-programmet har også fått mye kritikk fra Artikkel 29-gruppen. I sin rapport om Privacy Shield ordningen, som kom ut i november 2017, anbefalte Artikkel 29-gruppen å innføre endringer i 702-programmet.[9] På tross av Artikkel 29-gruppens og andre amerikanske personvernorganisasjoners anbefalinger ble likevel 702-programmet forlenget, uten endringer, i seks nye år etter en avstemning i den amerikanske kongressen den 18. januar i år.[10] Dette kan spille en viktig rolle for EU-domstolens vurdering av gyldigheten til SCCs når den tid kommer.

Når spørsmålene fra irsk høyesterett skal behandles i EU-domstolen vil derfor trolig amerikansk rett bli en stor del av saken. Dommer

5 Sak C-362/14 Schrems v. Data Protection Commissioner, 6. oktober 2015, ECLI:EU:C:2015:650 (Schrems)

6 Charter of Fundamental Rights of the European Union, 26. oktober 2012, OJ C 326

7 The High Court Commercial, The Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, 3. oktober 2017, 2016 No. 4809 P.

8 Foreign Intelligence Surveillance Act ("FISA""), Section 702, 50 U.S.C. § 1881 a

9 Artikkel 29-gruppen, EU-US Privacy Shield – First Annual Joint Review, 28. November 2017, 17-EN WP255

10 S139, An Act to amend the Foreign Intelligence Surveillance Act of 1978 to improve foreign intelligence collection and the safeguards, accountability, and oversight of acquisitions of foreign intelligence, to extend title VII of such Act, and for other purposes, 115th Congress (2017-2018) Public Law No: 115-118.

Costello antydet at spørsmålene kunne innebære en omfattende vurdering av amerikansk rett, herunder en vurdering av tilgjengelige rettsmidler i USA for personvernkrenkelser, analyser av amerikansk personvernrett og amerikansk regulering av elektronisk overvåkning. Den nylige vedtatte videreføringen av 702-programmet må antas å ha svekket muligheten for at SCCs overlever som overføringsgrunnlag, og det kan samtidig også vise seg å være spikeren i kisten for Privacy Shield.

Den usikre fremtiden til privacy shield

Privacy Shield er som kjent etterkommeren til Safe Harbour.[11] Det er et selvsertifiseringsregime der amerikanske selskaper sertifiseres for å kunne motta europeiske personopplysninger. Siden 2016 har Privacy Shield fungert som en praktisk overføringsmekanisme mellom USA og Europa, og per dags dato er over 2 700 amerikanske selskaper sertifisert.[12] Likevel har Privacy Shield møtt mye motbør og kritikk den siste tiden, både fra Artikkel 29-gruppen og fra andre personvernorganisasjoner.

Artikkel 29-gruppen gjennomførte i fjor høst sin første gjennomgang av Privacy Shield. Ordningen besto prøven, men Artikkel 29-gruppen presenterte en rekke kritiske punkter i sin rapport som de fastsatte at måtte bli håndtert innen 25. mai 2018. Artikkel 29-gruppen truer med å gå til rettslige skritt hvis ikke gruppens anbefalinger er tatt til følge innen innføringen av GDPR. I rapporten trekkes det blant annet frem at det fremdeles ikke er oppnevnt en Ombudsmann for Privacy Shield, og at det fremdeles er ledige stillinger som skal fylles i Privacy and Civil Liberties Oversight Board. Overvåkningen etter 702-programmet kritiseres som nevnt også og nå som dette programmet er videreført i seks år har sjansen økt for at Artikkel 29-gruppen gjør virkelighet av sine trusler om rettslige skritt mot Privacy Shield.

> Det er fremdeles ikke er oppnevnt en Ombudsmann for Privacy Shield

I tillegg har Privacy Shield blitt angrepet av to europeiske personverngrupper som også krever at ordningen er ugyldig. I Frankrike har tre organisasjoner: La Quadrature du Net, French Data Network og Federation FDN, gått sammen for å ugyldiggjøre ordningen. Den irske personverngruppen Digital Rights Ireland har forsøkt det samme, men tapte nylig i EU-domstolen, da domstolen fant at DRI som organisasjon ikke hadde rettslig interesse.[13] Det er nærliggende å anta at deres franske kollegaer vil møte med den samme skjebnen. Likevel er det også grunn til å tro at sjansene for suksess vil øke betraktelig etter 25. mai. Etter artikkel 80 i GDPR kan ideelle organisasjoner ha en mulighet til å saksøke for brudd på forordningen.[14] Organisasjonene må pent vente til 25. mai før de kan forsøke seg igjen under denne fanen og mye tyder på at de på implementeringsdatoen for GDPR ikke vil være alene om å kjempe om en plass i rettssystemet.

Max Schrems har naturlig nok allerede opprettet sin egen organisasjon, med det passende navnet NOYB (None Of Your Business). Schrems tapte for øvrig en sak om rettslig interesse i en Østerriksk domstol i januar, da domstolen fant at han ikke kunne føre et gruppesøksmål mot Facebook på vegne av de 25 000 forbrukerne han hadde samlet.[15] Betydningen av denne avgjørelsen er trolig ikke stor da Schrems fikk lov til å fremme søksmålet på vegne av seg selv. Det kan også stilles spørsmål ved om han nå muligens venter med dette søksmålet til 25. mai, da NOYB vil ha muligheten til å føre personvernsaker for europeiske domstoler.

Balkaniseringen av internett

På tross av at GDPR er en stor og viktig seier for personvernet er det liten tvil om at GDPR utgjør en felles europeisk hindring for internasjonal dataflyt. I tillegg er det nå en forholdsvis stor sannsynlighet for at både SCCs og Privacy Shield blir ugyldige som grunnlag for overføring av personopplysninger til USA. Dette vil skape enda flere hinder. Det finnes flere alternative overføringsgrunnlag i GDPR, men det er liten tvil om at ugyldiggjøringen av disse to ovennevnte ordningene kan lede til at opplysninger ikke kan overføres til USA eller tredjeland overhodet, med mindre tredjelandet kan vise at de følger prinsippene nedfelt i europeisk personvernlovgivning. Der avgjørelsen til Safe Harbour var begrenset til å vurdere denne spesifikke ordningen, er spørsmålet i Schrems 2, i et nøtteskall, hvorvidt EUs fundamentale rettigheter og gjeldende personvernlovgivning overhodet tillater å overføre personopplysninger til andre land uten adekvat beskyttelse. Sva-

11 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207

12 https://www.privacyshield.gov/list

13 Sak T 670/16 Digital Rights Ireland Ltd v European Commission, 22. november 2017, ECLI:EU:T:2017:838

14 Regulation (EU) 2016/679 artikkel 80

15 Sak C498/16 Maximilian Schrems v Facebook Ireland Limited, 25. januar 2018, ECLI:EU:C:2018:37

ret på det, i hvert fall når det kommer til USA, er trolig nei, all den tid 702-programmet får leve videre i 6 nye år.

Et slikt resultat vil i en periode utvilsomt ha mye å si for den internasjonale digitale økonomien, ikke bare for forholdet mellom USA og Europa. Likevel har overføring av data til andre steder enn USA foreløpig ikke vært høyt på agendaen for europeiske personvernforkjempere. Det har derfor fått forholdvis lite oppmerksomhet at Kina, kanskje noe overraskende, har innført sin egen personvernlov. Loven er den første i landets historie og innebærer at alle kinesiske personopplysninger skal lagres i Kina. Dette har blant annet fått som konsekvens at Apple har annonsert at de vil overføre ansvaret for driften av iCloud for kinesiske brukere, til det statlig eide selskapet GCBD i februar i år.[16] Kinesiske brukere som ikke ønsker at myndighetene skal få tilgang på deres opplysninger må avslutte sitt abonnement. I tillegg innebærer loven at myndighetene skal kunne gjennomføre sikkerhetsrevisjoner på produkter og teknologi av hensyn til nasjonal sikkerhet, og brudd på loven kan resultere i svært høye bøter. Man kan således trekke visse parallelle til både GDPR og USAs 702-program. Kinesiske myndigheters motivasjon for å innføre den nye personvernloven kan trolig diskuteres, men det er liten tvil om at loven innebærer nok en hindring for den internasjonale dataflyten.

> President Trumps næringsvennlige regjering har kommet på banen.

Det at viktige handelspartnere som EU og Kina har egne lover om personvern har ført til at president Trumps næringsvennlige regjering har kommet på banen. I følge «Cyber Security Coordinator» i det Hvite hus, Rob Joyce, har USA reagert sterkt på det de beskriver som en «fragmentering og balkanisering av internett».[17] Vi er bekymret for det lappeteppet av ulike regler som påvirker våre muligheter til å flytte data, uttalte Joyce i et intervju i januar. Joyce har blitt sitert på at USA vil involvere seg ytterligere i å få på plass internasjonale reguleringer av dataflyt for å sikre færre utfordringer for multinasjonale amerikanske selskap og ikke minst for amerikanske myndigheter. Denne uttalelsen kommer bare uker før det er ventet en avgjørelse i Microsoft-saken, der det vil komme en avklaring på hvorvidt amerikanske myndigheter kan få tilgang til amerikanske selskapers data som ikke er lagret på amerikansk jord.

Det kan bli interessant å se om de økonomiske konsekvensene av GDPR og utfallet av Schrems-sakene endelig får USA til å tenke nytt om viktigheten av personvern. Hvis resultatet isteden blir at USA ved Trump bestemmer at opplysninger om amerikanere ikke kan overføres til Europa, blir kaoset virkelig komplett. Hvis ikke Kina, USA og Europa kan enes om noen internasjonale prinsipper for dataflyt og personvern vil trolig den økonomiske effekten bli betydelig. På den annen side, hvem skal få bestemme hvilke personvernprinsipper som skal gjelde? I skjæringspunktet mellom nasjonenes sikkerhetspolitikk og behovet for personvern kan det vise seg å bli svært vanskelig å finne et minste felles multiplum. Det kan etter dette ikke råde særlig tvil om at 2018 blir et mildt sagt spennende år for personvernet.

Eva Jarbekk er partner i Schjødt.
Anne-Marit Wang Sandvik er advokat i Schjødt.

16 http://money.cnn.com/2018/01/10/technology/apple-china-icloud/index.html

17 https://www.cyberscoop.com/trump-international-data-laws-rob-joyce/

Personvernforordningen som endelig farvel til samtykke som preferert behandlingsgrunnlag

av Ove André Vanebo
og Hanne Jahr Pedersen,
Kluge Advokatfirma AS

Ove André Vanebo (Foto: Justis- og beredskapsdepartementet)

Hanne Jahr Pedersen

1 Artikkelens problemstilling

All behandling av personopplysninger som skjer med elektroniske hjelpemidler eller skal inngå i et personregister, er i utgangspunktet forbudt, med mindre det foreligger et rettslig grunnlag.

I personopplysningsloven («popplyl.») omtales rettslige grunnlag – såkalte «behandlingsgrunnlag» –, som «*vilkår for å behandle personopplysninger*», og er nedfelt i lovens §§ 8 og 9. Popplyl. § 8 fastslår at personopplysninger «*bare [kan] behandles dersom den registrerte har samtykket, eller det er fastsatt i lov at det er adgang til slik behandling, eller behandlingen er nødvendig for*» spesifikke grunner nevnt i loven. Det er altså tre behandlingsgrunnlag: 1. samtykke, 2. lovbestemt adgang, eller 3. en nærmere angitt nødvendighetsgrunn i § 8 bokstavene a-f.

Det har i personopplysningslovens virketid vært en rådende oppfatning om at samtykke er det foretrukne behandlingsgrunnlaget. Datatilsynet hevder at: «Når verksemder handsamar personopplysningar, skal dei i størst mogleg grad basere det på samtykke. Det inneber at du godtek at verksemda behandlar personopplysningar om deg.»[1]

25. mai 2018 gjennomføres EUs personvernforordning (2016/679) i norsk rett. Artikkelens hovedproblemstilling er om den nye personvernforordningen viderefører oppfatningen av at samtykke skal være hovedregelen, dvs. det prefererte utgangspunktet ved valg av grunnlag for behandling av personopplysninger. Justisdepartementets høringsutkast hevder at personvernforordningens løsning «*på dette punktet i stor grad [svarer] til gjeldende rett*».[2] Det er derfor relevant å gjennomgå hva som må anses som gjeldende rett på nåværende tidspunkt. Etter vårt skjønn viser rettskildebildet at det er tvilsomt om samtykke er det foretrukne behandlingsgrunnlag *de lege lata*, se punkt 3-7 og 9.

Problemstillingen kan i utgangspunktet virke teoretisk, men skaper i praksis flere utfordringer. De fleste aktører i næringsliv og offentlig sektor behandler personopplysninger. Oppfatningen om at samtykke må vurderes før nødvendighetsgrunnene, medfører ofte at det gjøres inngående analyser for å finne ut om samtykke er et passende grunnlag for en behandling – til tross for at det ville vært kurant å benytte et annet grunnlag. Dette synspunktet utdypes i punkt 2.

2 Hvorfor er det problematisk å benytte samtykke som grunnlag for behandling av personopplysninger?

Etter popplyl. § 2 nr. 7 er et samtykke «*en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv*». Dette svarer i stor grad til forordningens definisjon i artikkel 4 nr. 11, som slår fast at et samtykke er

1 Datatilsynets nettsider: *https://www.datatilsynet.no/om-personvern/samtykke/* [Pr. 18. januar 2018]

2 Justis- og beredskapsdepartementet, Høringsnotat, Snr. 17/4200; Ny personopplysningslov – *Gjennomføring av personvernforordningen i norsk rett,* 6. juli 2017 s. 24 (heretter omtalt som «høringsnotatet»).

any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[3]

Kravene til et gyldig samtykke skaper utfordringer i praksis. Det er ofte uklarheter knyttet til hvorvidt den registrerte har fått tilstrekkelig informasjon, eller hva vedkommende *uttrykkelig* (gjenspeiles i kriteriene «specific» og «unambiguous»)[4] har samtykket til. De største utfordringene knytter seg imidlertid til at samtykket må være avgitt frivillig.

Ulike former for tvangssituasjoner gjør naturligvis at samtykket ikke anses «frivillig».[5] Det er videre antatt at et samtykke neppe er gyldig dersom det vil «*få en negativ følge for personen dersom samtykke nektes*»[6]. Det er dessuten lagt til grunn i teori at et samtykke også vil «*kunne trekkes i tvil dersom det knyttes for positive følger til det å samtykke, for eksempel der hvor et samtykke belønnes med en gave av stor verdi*».[7] Det er heller ikke nødvendig at det *faktisk* får betydning for en person om samtykke gis eller ikke for å trekke frivilligheten i tvil – det er tilstrekkelig at *tanken melder seg*, jf. Personvernnemndas avgjørelse PVN 2005-6.

Dette medfører at samtykker ofte er upraktiske som rettslige grunnlag for behandling av personopplysninger.

> I all hovedsak vil forordningen videreføre innholdet i kravene til gyldig samtykke, og dermed vil de samme problemstillingene gjøre seg gjeldende også med den nye reguleringen.

I all hovedsak vil forordningen videreføre innholdet i kravene til gyldig samtykke, og dermed vil de samme problemstillingene gjøre seg gjeldende også med den nye reguleringen.[8] I forordningen punkt 42 heter det bl.a. at «*[c]onsent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment*». I tillegg kan ubalanse mellom parter medføre at samtykke fra den registrerte ikke er gyldig, f.eks. ved samtykke fra de ansatte før kontrolltiltak settes i gang av arbeidsgiver, jf. fortalepunkt 43.

3 Personopplysningslovens ordlyd

3.1 Fortolkning av ordlyden

Loven oppstillinger ingen klar rekkefølge eller rangering av de ulike rettslige grunnlagene for behandling av personopplysninger, se punkt 1. Det kan kanskje oppfattes som at samtykke skal være hovedregelen fordi dette nevnes først. Samtidig kan bruken av ordet «eller» indikere at de ulike grunnlagene kun er nevnt som alternative grunnlag, og at det således er opp til den behandlingsansvarlige å avgjøre hvilket grunnlag som skal anvendes. Lovens ordlyd gir etter vår mening ikke grunnlag for en prioritering mellom de ulike rettsgrunnlagene.

Juridisk teori som drøfter hvordan lovens ordlyd må forstås, påpeker også at bestemmelsens formuleringer neppe gir grunnlag for en prioriteringsrekkefølge. Eksempelvis skriver *Wiese Schartum* og *Wick Sætre* at: «*Loven inneholder ikke noen prioriteringsregler mellom de ulike typene rettslige grunnlag, og det kan derfor være uklart hva som kan/skal/bør velges.*»[9]

3.2 Tilsier personopplysningslovens formål at samtykke er et preferert behandlingsgrunnlag?

Popplyl. § 1 første ledd slår fast at «*[f]ormålet med denne loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger*». Loven skal også bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, jf. annet ledd.

Coll og *Lenth* mener at «*[l]oven må forstås slik at den behandlingsansvarlige i størst mulig grad bør basere behandlingen på et samtykke*», og hevder dette «kan forankres i lovens formålsbestemmelse i § 1».[10]

---

3 Høringsnotatet s. 40 slår fast at «*[f]orordningen viderefører i det vesentlige gjeldende rett om kravene til et gyldig samtykke, samtidig som kravene er noe utdypet og presisert*».

4 Ot.prp.nr. 92 (1998-1999) s. 103 og høringsnotatet 2017 s. 41.

5 Dag Wiese Schartum og Lee Bygrave, *Personvern i informasjonssamfunnet; En innføring i vern av personopplysninger, 3. utgave 2016,* s. 178, Michal Wiik Johansen, Knut-Brede Kaspersen og Åste Marie Bergseng Skullerud, Personopplysningsloven; Kommentarutgave, 2001, s. 77.

6 Note 14 til personopplysningsloven i Gyldendal Rettsdata ved Dag Wiese Schartum (2012).

7 Christine Ask Ottesen og Katrine Berg Blixrud, *Personvern i finanssektoren,* 2010, s. 72.

8 Høringsnotatet s. 40-41.

9 Dag Wiese Schartum og Kjetil Wick Sætre, *Samtykke til å behandle personopplysninger i offentlig forvaltning,* Complex nr. 2, Oslo 2016, s. 20. Se også Elisabeth Krauss Amundsen, *Prioriteringsrekkefølge mellom de rettslige grunnlagene i personopplysningsloven* § 8, CompLex 1/2016, Oslo 2016, s. 33-34, som mener at «proposisjonen ikke kan tas til inntekt for at lovgiver har ment at det gjelder en prioriteringsrekkefølge mellom samtykke fra den registrerte og nødvendighetsgrunnene i personopplysningsloven § 8».

10 Line M. Coll og Claude A. Lenth, *Personopplysningsloven – en håndbok,* Oslo 2000, s. 42

Slik vi leser formålsbestemmelsen, vil denne i all hovedsak få betydning ved tolkningen av hvilke opplysninger som faller inn under lovens saklige virkeområde og i forbindelse med skjønnsmessige interesseavveininger ved behandling av personopplysninger.[11] Selv om selvbestemmelse over egne opplysninger kan sies å falle inn under *grunnleggende personvernhensyn*, vil ivaretakelse av personvernet i mange situasjoner tilsi at den registrerte *ikke* bør kunne frasi seg vern gjennom et samtykke, jf. punkt 2. Forarbeidene understreker at det ved tolkningen av lovens øvrige bestemmelser, er «*naturlig å legge vekt på hovedsiktemålet om å verne mot krenkelse av den personlige integritet*».[12] Det synes derfor som om lovens § 1 *ikke* forankrer en preferert stilling for samtykket i § 8.

4 Forarbeidenes uttalelser

4.1 Lovproposisjonen

Departementet mente i Ot.prp. nr. 92 (1998-1999) s. 108 at det var «*viktig å få lovfestet generelle behandlingsvilkår, som f. eks krav om samtykke*». Videre fremholdt departementet at «*[b]ehandling av personopplysninger bør i størst mulig utstrekning baseres på samtykke fra den registrerte, selv om den også kan hjemles i de grunnlagene som oppstilles i bokstavene a-f*».

Datatilsynet har på bakgrunn av uttalelsen oppfattet at samtykke har en stilling som preferert grunnlag. Det samme har tradisjonelt blitt lagt til grunn i praksis fra Personvernnemnda og i juridisk teori, se punkt 5 og 7.

Hva departementet mente med uttrykket «bør» er imidlertid ikke presisert. Det kan hevdes at formuleringen «bør» ikke gir uttrykk for en rettslig bindende norm,[13] men snarere indikerer hva som er hensiktsmessig og praktisk.[14]

Hvorfor samtykkets særstilling verken er lovfestet eller tydeliggjort i forarbeidene fremkommer ikke av proposisjonen. Departementet drøfter heller ikke hvordan samtykkets eventuelle prefererte stilling forholder seg til personverndirektivets løsning. Videre fremstår det som uklart hva departementet mener med at behandlingen «*også kan hjemles i de grunnlagene som oppstilles i bokstavene a-f*». En slik formulering kan like gjerne oppfattes som om at det er valgfritt hvilket grunnlag den behandlingsansvarlige ønsker å benytte. Hvilke konsekvenser det ev. får at behandlingsansvarlig hjemler behandling i nødvendighetsgrunnene uten å vurdere samtykke først, er ikke nevnt.

> Med andre ord kan det etter vår mening settes spørsmålstegn ved oppfatningen om at forarbeidene angir samtykke som det prefererte grunnlag og lovens hovedregel

Med andre ord kan det etter vår mening settes spørsmålstegn ved oppfatningen om at forarbeidene angir samtykke som det prefererte grunnlag og lovens hovedregel, se punkt 7.

Forarbeidenes begrunnelse for at samtykket kan synes å ha en preferert stilling er todelt: Dels at et samtykke «*vil […] styrke den registrertes muligheter til å råde over opplysninger om seg selv*», og dels i det praktiske ved at samtykke reduserer tvil om lovlighet, sammenlignet med å anvende mer skjønnsmessige nødvendighetsvilkår.[15] Etter vårt skjønn, fremstår begrunnelsene som tynne, noe som svekker uttalelsenes vekt.

For så vidt gjelder poenget om å styrke den registrertes råderett, er det som nevnt vår oppfatning at det sjelden er anledning til å samtykke når det er tale om viktige beslutninger, jf. artikkelens punkt 2. Dette gjelder f.eks. når det er tale om ev. samtykke til arbeidsgivers kontrolltiltak. Dermed kan råderetten få redusert betydning.

For det annet mener vi at samtykke heller ikke er egnet til å redusere tvilen som melder seg ved spørsmålet om riktig behandlingsgrunnlag. Som vi tok opp i punkt 2, er det ofte vanskelig å vite om samtykket er tilstrekkelig presist, informert eller frivillig.

5 Personvernnemndas praksis

I personvernnemndas klagesak 2004/1 var det sentrale spørsmålet om det skulle kreves samtykke fra de registrerte for å tillate en oppfølgingsstudie, eller om studien kunne forankres i en av nødvendighetsgrunnene i §§ 8 og 9, jf. popplyl. § 11. Statens arbeidsmiljøinstitutt ønsket å gjennomføre oppfølgingsstudien om kreft og lungesykdommer blant ansatte i en bestemt industri.

Nemnda trakk frem det «*forhold at samtykke er hovedregelen*», og presiserte at den behandlingsansvarlige «*kan avvike fra dette prinsippet, og i stedet bygge på en av nødvendighetsbegrunnelsene i personopplysningsloven § 8*». Det betyr imidlertid ikke at den behandlingsansvarlige «*står fritt til å velge en nødvendighetsbegrunnelse av rene hensiktsmessighetsbetraktninger*». For å fravike hovedregelen kreves at den behandlingsansvarlige hensyntar det «*prinsipielle og formelle syn at loven må forstås slik at samtykke skal prioriteres*» og ser disse opp mot «*de konkrete argumentene for å velge nødvendighetsbegrunnelse, og hvor tungt-*

11 Ot.prp. nr. 92 (1998-1999) s. 101, Wiik Johansen, Kaspersen og Bergseng Skullerud 2001 s. 66 og Wiese Schartum og Bygrave 2016 s. 130-131.

12 Ot.prp. nr. 92 (1998-1999) s. 101.

13 Se til eksempel Personvernnemndas uttalelse PVN-2012-1.

14 Krauss Amundsen 2016 s. 33.

15 Ot.prp. nr. 92 (1998-1999) s. 108.

veiende de er i den konkrete sak». Poenget er, ifølge nemnda, at avvik forutsetter at det «*må […] foreligge en begrunnelse», som «må vurderes konkret i forhold til den enkelte sak*».

Nemnda finner støtte for sin oppfatning i personopplysningslovens forarbeider, ordlyden i helseregisterloven § 5 første til tredje ledd, og forståelsen av personvernets innhold slik det kommer til uttrykk i den gamle personregisterloven og personverndirektivet.

Oppfatningen er fulgt opp i nemndas senere saker. Eksempelvis er det i vedtak 2007/7 sagt at «*[h]ovedregelen etter personopplysningsloven § 8 er at behandling av personopplysninger skal bygge på samtykke fra den regist[r]erte*». En rekke andre saker inneholder lignende formuleringer.[16]

Nemnda foretok imidlertid en overraskende vending i avgjørelsen PVN-2012-1. Avgjørelsen gjaldt om det forelå behandlingsgrunnlag for en rettsmedisinsk studentoppgave. I vedtaket tar nemnda avstand fra Datatilsynets tidligere standpunkt om «*at behandlingsgrunnlag som hovedregel skal være samtykke*». Nemnda bemerket «*at etter en naturlig språklig forståelse av lovteksten i personopplysningsloven § 8 fremstår de ulike behandlingsgrunnlagene […] som likeverdige*».

Selv om forarbeidene fremhever at man «bør» forsøke å innhente samtykke, mente nemnda at forarbeidenes uttalelse «*anses ikke som en rettslig normering, men som en hensiktsmessighetsbetraktning*» – med den konsekvens at «*de ulike behandlingsgrunnlagene derfor behandles som likestilte*». For øvrig viste nemnda til at personverndirektivets artikkel 7 og Peter Blumes fagtekst «*Vurdering af Personvernnemndas praksis 2001-2008*», tilsa at nemnda tidligere hadde lagt for stor vekt på samtykke som grunnlag for behandling av personopplysninger.

16 Blant annet klagesakene 2004/2, 2005/8, 2005/9 og 2005/10.

Nemnda har ikke uttalt seg om problemstillingen etter PVN-2012-1.

6 Personverndirektivets løsning

6.1 Innledende om direktivet

Bestemmelsen i popplyl. § 8 implementerer artikkel 7 i personverndirektivet.[17] Kilder fra EU- og EØS-retten er derfor relevant ved kartleggingen av bestemmelsens innhold. Artikkel 7 fastslår at «*[m]edlemsstatene skal fastsette bestemmelser om at behandling av personopplysninger kan utføres bare dersom*» et nærmere vilkår i bokstavene a-f er oppfylt. At «*den registrerte har gitt sitt utvetydige samtykke*» er nevnt i bokstav a, men det står ingenting om en foretrukket rekkefølge.

> Ut fra en naturlig språklig forståelse av direktivet er det altså ingen prioriteringsrekkefølge mellom de ulike grunnlagene. Det samme er lagt til grunn i juridisk teori.

Ut fra en naturlig språklig forståelse av direktivet er det altså ingen prioriteringsrekkefølge mellom de ulike grunnlagene. Det samme er lagt til grunn i juridisk teori.[18]

Etter EØS-retten skal myndighetene benytte EØS-rettslige tolkningsprinsipper når EØS-retten kommer til anvendelse. Nasjonale rettsregler innenfor EØS-rettens anvendelsesområde skal tolkes EØS-konformt.[19] Selv om proposisjonen viser til at § 8 gjennomfører artikkel 7, er det ikke problematisert hvordan artikkelen forholder seg til harmonisering i EØS-/EU-området.[20] Departementet konstaterer enkelt at «*[i]nnledningsvis slås det fast at behandlingen kan finne sted dersom den registrerte har samtykket, jf. også artikkel 7 bokstav a i EU-direktivet*».[21]

Interessant nok ble prioriteringsrekkefølge mellom grunnlagene berørt i St.prp. nr. 34 (1999-2000), om samtykke til godkjenning av EØS-komiteens beslutning nr. 83/1999 av 25. juni 1999. På side 2 i proposisjonen er det påpekt at «*[f]orslag til lovendringer for å gjennomføre beslutningen er forelagt Stortinget ved Ot. prp. nr. 92 (1998-1999) […]. Stortinget inviteres gjennom denne proposisjonen til å samtykke til godkjenning av EØS-komiteens beslutning*». Om direktivets artikkel 7, som inneholder behandlingsgrunnlagene, heter det at «*[b]estemmelsen oppstiller uttømmende vilkår for at behandlingen av personopplysninger kan finne sted. Vilkårene er alternative, slik at det er tilstrekkelig at ett av dem er oppfylt.*»[22]

Personverndirektivet er EØS-relevant og dermed folkerettslig bindende for Norge. Personopplysningsloven gjennomfører personverndirektivet i Norge. I EU-rettspraksis kan det synes som om direktivet i stor grad vil medføre krav om ensartet gjennomføring av reglene for behandlingsgrunnlag. I EF-domstolens sak C-101/01 (Bodil Lindquist) avsnitt 96, er det uttalt at direktivet legger opp til en harmonisering som i prinsippet er fullstendig. EU-domstolen avsa 24.

17 Personverndirektivet er direktiv 95/46/EF. I forarbeidene heter det følgende om popplyl. § 8: *«Bestemmelsen, som gjennomfører EU-direktivet artikkel 7», slår fast «at behandlingen kan finne sted dersom den registrerte har samtykket, jf. også artikkel 7 bokstav a i EU-direktivet»,* se Ot.prp. nr. 92 (1998-99) s. 108.

18 Wiese Schartum og Bygrave 2016 s. 183 og Krauss Amundsen 2016 s. 14.

19 Bjørnar Alterskjær og Niels Fenger, *«EØS-rettens betydning for norsk forvaltningsrett»,* Jussens Venner 2006, s. 171–192, på s. 173.

20 Ot.prp. nr. 92 (1998-99) s. 108

21 l.c.

22 St.prp. nr. 34 (1999-2000) s. 4-5.

november 2011 dom i to forenede saker, C-468/10 og C-469/10, som gjaldt forståelsen av direktivets artikkel 7 bokstav f. Reguleringen korresponderer med personopplysningsloven § 8 bokstav f, som gir grunnlag for behandling av personopplysninger etter en interesseavveining. Spansk lovgivning hadde stilt opp som et tilleggsvilkår for lovlig behandling at opplysningene måtte være oppført i offentlig tilgjengelige kilder.

Dommens avsnitt 32 slår fast at medlemsstatene «*verken kan tilføye nye prinsipper vedrørende grunnlaget for behandling av opplysninger i artikkel 7 i direktiv 95/46, eller fastsette supplerende krav, som endrer rekkevidden av et av de seks prinsipper som er fastsatt i denne artikkel. [Vår oversettelse]*». Bakgrunnen for denne oppfatningen er at artikkel 7 inneholder formuleringen «*behandling av personopplysninger kan utføres bare dersom*», se avsnitt 31.[23]

Vi vil også fremheve at personverndirektivet har flere begrunnelser, i tillegg til rent idealistiske personvernverdier. Det skal også sikre uniforme rettsregler, som kan sørge for velfungerende markeder og friere utveksling av personopplysninger, samt understøtte felles forvaltningsordninger.[24] Dersom spillerommet blir stort for ulike behandlingsgrunnlag, kan det stilles spørsmål ved om behandlingene hviler på et tilfredsstillende rettslig grunnlag. Etter dette mener vi at gode grunner taler for at en løsning med samtykke som preferert behandlingsgrunnlag kan være i strid med EØS-rettslige forpliktelser.[25]

6.2 Artikkel 29-gruppens tolkning av direktivet

Artikkel 29-gruppen er et fellesorgan for EU/EØS-statenes tilsynsmyndigheter. Organets hovedoppgave er å gi råd til Kommisjonen om problemstillinger som berører felleseuropeiske personvernreguleringer, herunder forståelsen av direktivet og den nye forordningen. I flere uttalelser har gruppen uttalt seg om samtykkets status i forhold til de andre grunnlagene i direktivet.

En uttalelse fra 2011 berører definisjonen av samtykke etter direktivet.[26] I avsnittene som følger etter underoverskriften *Consent is not the only ground for lawfulness*, presiserer gruppen at: «*The order in which the legal grounds are cited under Article 7 is relevant, but it does not mean that consent is always the most appropriate ground to legitimize the processing of personal data.*»[27] Gruppen synes i den etterfølgende drøftelsen at det må vurderes i hvert enkelt tilfelle hvilket grunnlag som er passende Det er likevel uklart hva gruppen mener med formuleringen «*[t]he order in which the legal grounds are cited under Article 7 is relevant*».

Den andre uttalelsen fra 2014 gjelder bruk av interesseavveining som rettslig grunnlag. Uttalelsen nevner 2011-uttalelsen og bekrefter at samtykke ikke har en preferert stilling:

> *Consent as a legal ground has been analyzed in Opinion 15/2011 of the Working Party on the definition of consent. The main findings of the Opinion are that consent is one of several legal grounds to process personal data, rather than the main ground. It has an important role, but this does not exclude the possibility, depending on the context, that other legal grounds may be more appropriate either from the controller's or from the data subject's perspective.*[28]

2014-uttalelsen påpeker videre at «*the text of the Directive does not make a legal distinction between the six grounds and does not suggest that there is a hierarchy among them*».[29]

7 Juridisk teori

7.1 Generelt om oppfatningen i litteraturen

I eldre litteratur var det vanlig å forfekte at samtykke var det prioriterte behandlingsgrunnlaget. Lovkommentaren til personopplysningsloven hevder at «*[d]et er lovgivers intensjon at behandlingen av personopplysninger i størst mulig grad skal baseres på samtykke*».[30] Vi har ovenfor i punkt 3.2 nevnt at Coll og Lenth mener at lovens formålsbestemmelse tilsier at samtykke har en særstilling som behandlingsgrunnlag.[31] Andre har vært mer varsomme med å konkludere, men samtidig påpekt at det «*[g]enerelt er […] grunn til å vektlegge betydningen av samtykke og den enkeltes medvirkning og aksept*».[32]

I nyere juridisk litteratur kan vi spore stadig større skepsis til å hevde at samtykke er preferert behandlingsgrunnlag. Som allerede nevnt,

---

23 EU-domstolens sak C-582/14 fastholder oppfatningen om at medlemsstater *«cannot introduce principles relating to the lawfulness of the processing of personal data other than those listed in Article 7 thereof, nor can they amend, by additional requirements, the scope of the six principles provided for in Article 7»,* se avsnitt 58.

24 NOU 1997: 19 kapittel 8.1 og Alterskjær og Fenger 2006 s. 183.

25 Se også Bjarne Kvam, *Politiets persondatarett,* 2014 sidene 58-59.

26 Artikkel 29-gruppen, *Opinion 15/2011 on the definition of consent.*

27 Artikkel 29-gruppen 2011 s. 7.

28 Artikkel 29-gruppen, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC,* s. 16.

29 Artikkel 29-gruppen 2014 s. 10.

30 Wiik Johansen, Kaspersen og Bergseng Skullerud 2001 s. 97.

31 Line M. Coll og Claude A. Lenth s. 42.

32 Dag Wiese Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet; En innføring i vern av personopplysninger, 1. utgave,* 2004, s. 135-136.

påpekte *Blume* tidlig i sin gjennomgang av Personvernnemndas praksis at samtykkets betydning ikke måtte få en for fremtredende rolle.[33]

Skepsisen er mangefasettert. Den mer moderate skepsisen påpeker at «*[d]et kan stilles spørsmål ved om denne praksisen om [at samtykke er hovedregelen] har utviklet seg i en litt for kategorisk retning*».[34] I samme retning er uttalelser om at det er «*uklart om en behandlingsansvarlig kan nøye seg med å konstatere at kravet til nødvendighet er tilfredsstilt og derfor la være å innhente samtykke fra de personer opplysningene gjelder*».[35] Mer tydelige teoretikere hevder at man skal «*være forsiktig med å hevde at samtykke er en hovedregel som bør foretrekkes*», og at enkelte kilder foreskriver at samtykkets egnethet «*må vurderes konkret, og at det ikke er grunnlag for å trekke frem samtykke som en hovedregel fremfor de andre behandlingsgrunnlagene*».[36]

Wiese Schartum og *Wick Sætre* reiser spørsmålet om samtykke har prioritet fremfor andre grunnlag. De tiltrer den konklusjon at «*det på generelt grunnlag ikke kan sies å eksistere noen prioriteringsrekkefølge, men at valget mellom ulike rettslige grunnlag må tas på bakgrunn av forholdene i den konkrete situasjon behandlingen av personopplysninger skal foregå*».[37]

Bjarne Kvam går kanskje klarest ut mot forarbeidenes oppfatning om at samtykke skal foretrekkes fremfor andre grunnlag. Han viser til at oppfatningen om at samtykke «ble ansett som et preferert rettsgrunnlag», er en av «*flere regler som avviker fra [personvern]direktivet*», og dermed «*er i strid med EØS-rettens krav til harmonisering*».[38]

Også Elisabeth Krauss Amundsen hevder «*at det etter gjeldende rett ikke kan oppstilles noen fast prioriteringsrekkefølge mellom samtykke fra den registrerte og nødvendighetsgrunnene i personopplysningsloven § 8*».[39]

Oppsummert er det altså temmelig klart at nyere, juridisk teori taler i mot en hovedregel om samtykke som preferert behandlingsgrunnlag. Det kan synes som om flere tar til orde for at det må vurderes mer konkret hva slags grunnlag som er egnet i den aktuelle behandlingssituasjonen, snarere enn å operere med samtykke som en hovedregel.[40]

8 Personvernforordningens regulering

8.1 Forordningens ordlyd

EØS-avtalen art. 7 bokstav a) bestemmer at forordninger «som sådan» gjøres til del av vår interne rettsorden. Norge har dermed ikke den valgfriheten man hadde i implementeringen av det någjeldende direktivet ved gjennomføringen av den nye personvernforordningen.

> Samtykke er således bare er ett av flere mulige - og likestilte – grunnlag.

Forordningens art. 6 nr. 1 slår fast at «*[p]rocessing shall be lawful only if and to the extent that at least one of the following applies*», for deretter å ramse opp seks nærmere angitte grunnlag i bokstavene a til f. Bokstav a nevner at «*the data subject has given consent to the processing of his or her personal data for one or more specific purposes*».

Ut fra systematikken er en nærliggende oppfatning at det ikke er noen prioritering mellom de ulike grunnlagene. Samtykke er således bare er ett av flere mulige - og likestilte – grunnlag. I så måte er reguleringen tilsvarende som etter direktivets løsning,[41] som vi behandlet i punkt 6.

Også etter forordningen er det naturlig å tenke seg at ulike prinsipper vil styre hvilket grunnlag som er best egnet i det aktuelle tilfellet. Blant annet er det naturlig å tenke seg at samtykke i mange tilfeller bør velges for å sikre at personopplysninger «*behandles på en lovlig, rettferdig og gjennomsiktig måte*», jf. forordningens art. 5 nr. 1 bokstav a.[42] Dette er imidlertid noe annet enn å operere med en tilnærming om at et bestemt grunnlag som *hovedregel* skal foretrekkes fremfor andre.

8.2 Andre kilders forståelse av forordningen

Foreløpig er det et begrenset rettskildemateriale som uttaler seg om hvordan forordningen må forstås for så vidt gjelder samtykkets stilling som behandlingsgrunnlag. De spredte kildene som finnes, trekker likevel i retning av at samtykke bare er ett av flere alternative behandlingsgrunnlag:

Justisministeriets betenkning

De danske forarbeidene til implementeringen av forordningen påpeker at forordningen «*indeholder en tilsvarende bestemmelse [som den danske persondataloven] om, hvornår behandlingen af almindelige ikke-følsomme oplysninger må finde sted*». Ifølge de samme forarbeidene innebærer dagens regulering i persondataloven at «*de forskellige hjemler […] er sidestillede, og*

33 Peter Blume, *Vurdering af Personvernnemndas praksis 2001-2008,* Complex nr. 3/2009, Oslo 2009, s. 13.
34 Ask Ottesen og Berg Blixrud 2010 s. 86.
35 Note 35 i Gyldendal Rettsdata Norsk Lovkommentar ved Dag Wiese Schartum (2012).
36 Tønseth, Stubø, Olsen og Ljostad 2016 s. 27-28.
37 Wiese Schartum og Wick Sætre 2016 s. 20.
38 Kvam 2014 s. 59.
39 Krauss Amundsen 2016, s. 57.
40 I tillegg til de som er nevnt, se også Wiese Schartum og Bygrave 2016 s. 184, og Berg Blixrud og Ask Ottesen s. 86-87
41 SOU 2017: 39 s. 104 slår fast at: «*Artikel 6.1 i dataskyddsförordningen motsvarar i stora drag artikel 7 i dataskyddsdirektivet …*».
42 Blume 2016 s. 63-64.

behandlingen af personoplysninger er hjemlet, hvis blot én du af de 7 hjemmelsgrundlag er opfyldt».[43] Et annet sted i forarbeidene hevdes at «*[f]orordingens ses at have samme systematik som … databeskyttelsesdirektivet*» på dette området.[44]

Juridisk teori

Dansk juridisk teori taler for at samtykke ikke har en preferert stilling. *Peter Blume* mener at samtykke «*blot er en af flere alternative behandlingsbetingelser, som den dataansvarlige frit kan vælge imellem. Der er således ikke tale om en hovedregel*».[45] I annen litteratur påpeker Blume at «*[b]ehandlingsbetingelserne er alternative, og den dataansvarlige kan sædvanligvis vælge frit*».[46] Han hevder videre at forordningens regulering av samtykkebruken ikke skal gi den registrerte «*eksklusiv kontrol*»,[47] og at forordningen «*indicerer … at det er ønskeligt, at samtykke benyttes i begrænset omfang*».[48]

Paul Voigt og *Axel von dem Bussche* behandler ikke eksplisitt spørsmålet om samtykkets eventuelle prefererte status, men hevder i sin redegjørelse at: «*[E]ntities should - prior to processing - evaluate which legal basis might be most suitable for their processing activities*».[49] Etter vårt skjønn er denne tilnærmingen i tråd med hva vi mener er gjeldende rett, dvs. at det må gjøres en konkret vurdering i hvert enkelt tilfelle.

Myndighetspraksis

Det danske Datatilsynet og Justisministeriet sier i sin veiledning at «*[s]amtykke er efter databeskyttelsesforordningen […] et af flere – ligestillede – behandlingsgrundlag, som den dataansvarlige kan anvende ved behandling af personoplysninger*».[50]

Også det britiske datatilsynets utkast til veiledning om bruken av samtykke, påpeker at «*consent is one of [six lawful bases listed in Article 6(1)]*».[51] Videre slås det fast at «[c]onsent won't always be the easiest or most appropriate», og at valget av grunnlag må bero på valg av «*the lawful basis that most closely reflects the true nature of your relationship with the individual and the purpose of the processing*».[52] Videre sies at samtykke *må* brukes «*when no other lawful basis applies*».[53]

Artikkel 29-gruppen

I en foreløpig uttalelse om samtykke etter den nye forordningen, synes det som om Artikkel 29-gruppen viderefører oppfatningen om at samtykke bare er ett av flere likestilte grunnlag. Gruppen forklarer at samtykke «*remains one of six lawful bases to process personal data, as listed in Article 6 of the GDPR*». Videre heter at behandlingsansvarlig alltid må vurdere «*whether consent is the appropriate lawful ground for the envisaged processing or whether another ground should be chosen instead*».[54]

9 Avsluttende merknader

Det er uklart om Justisdepartementet mener at den nye forordningen innebærer at løsningen om samtykke som preferert grunnlag skal eller bør videreføres. Også Datatilsynets høringssvar til departementet etterlater tvil, idet svaret slår fast at «*[f]orordningen viderefører i det vesentlige gjeldende rett*». Tilsynet nevner også at i «*hvilken grad den enkelte borger selv er gitt rett til å bestemme over bruken av egne opplysninger, er […] sentral i vurderinger som gjelder om en bestemt behandling kan bygge på et annet rettslig grunnlag enn samtykke*».[55] Formuleringene skaper et inntrykk av at det må foreligge tungtveiende grunner for å kunne fravike samtykke som grunnlag. Som vår gjennomgang viser, er det imidlertid tvilsomt om samtykke skal anses som preferert grunnlag.

Forordningen gjenspeiler personverndirektivets løsning, og vi mener også derfor at det ikke vil være mulig å anvende samtykke som et preferert grunnlag etter forordningens ikrafttreden i norsk rett 25. mai 2018. Prioriteringsrekkefølgen har ingen basis i EU-/EØS-retten, og det må derfor ha liten betydning hva Datatilsynet og Justisdepartementet måtte uttale om spørsmålet. Forordningen må – og bør – derfor være den siste spikeren i kista for samtykke som foretrukket behandlingsgrunnlag.

Ove André Vanebo er senioradvokat i Kluge Advokatfirma AS.
Hanne Jahr Pedersen er assosiert partner i Kluge Advokatfirma AS.

43 Justisministeriet, *Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning;* Betænkning nr. 1565, 2017 s. 113.
44 Justisministeriet 2017 s. 127.
45 Peter Blume, *Den nye persondataret; Persondataforordningen,* 2016 s. 64.
46 Peter Blume, *Persondataretlige grundfigurer; Strejftog i den nye persondataret,* 2017 s. 67.
47 Blume 2017 s. 47.
48 Blume 2017 s. 67.
49 Paul Voigt og Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR),* 2017 s. 101.
50 Datatilsynet og Justisministeriet, *Samtykke,* 2017 s. 4
51 Information Commissioner's Office Consultation, *GDPR draft consent guidance,* 2017 s. 9.
52 Information Commissioner's Office Consultation 2017 s. 11.
53 Information Commissioner's Office Consultation 2017 s. 12.
54 Artikkel 29-gruppen, *Guidelines on Consent under Regulation 2016/679,* 2017 s. 4. Frem til 23. januar 2018 kunne man sende inn kommentarer til uttalelsen.
55 Datatilsynet, *Høringsuttalelse fra Datatilsynet - utkast til ny personopplysningslov - gjennomføring av personvernforordningen i norsk rett,* 16. oktober 2017, s. 39.

Tre juridiska problemområden avseende blockchain

av David Frydlinger,
Advokatfirman Lindahl.

En revolutionerande teknik om ett bortglömd fenomen

Blockchain – eller blockkedjeteknik – har potential att förändra samhälle och ekonomi i nästan lika stor grad som artificiell intelligens. Bitcoin var bara det första steget i en omvälvande process vars konsekvenser vi inte kan överblicka. Därför är juridiken rörande blockchain viktig att analysera och följa. I denna korta artikel ger gör jag en snabb överflygning av tre viktiga juridiska problemområden avseende blockchain.

Blockchains revolutionära potential framstår inte som självklar vid första påseende. Jag skulle tro att detta beror på att tekniken påverkar och förändrar en grundbult i den kapitalistiska ekonomin som vi tar så för givet att vi glömmer den. Denna grundbult är *liggaren* – the ledger. Det är detta som blockchain handlar om. Liggaren är en förteckning som registrerar händelser i den ordning de inträffar. Typiskt sett, men inte alltid, rör det sig om registrering av ekonomiska transaktioner eller liknande händelser.

Ett företags bokföring sker i en liggare, nämligen huvudboken, där alla företagets transaktioner antecknas på två ställen i olika konton. Varulager har lagerliggare, där alla varor som går in och ut ur lagret registreras. Restauranger har personalliggare, där de anställdas arbetade tid registreras varje dag. Ett bankkonto är en liggare. En aktiebok också. Så också fastighetsregistret, bilregister, fartygsregister, varumärkesregister, patentregister osv. Ett otal liggare utgör – för att bli något filosofisk – en slags ekonomisk representation av den fysiska verkligheten. Den visar ett nuläge, t.ex. när det gäller vem som äger vad, och de historiska stegen som har lett till detta nuläge. Liggaren utgör, utan att man kanske tänker på det, en praktisk förutsättning för hela det juridiska äganderättssystemet och detta system utgör i sin tur den grundpelare som en kapitalistisk ekonomi vilar på.

David Frydlinger

Blockchain-teknologin benämns också ”distributed ledger technology”, vilket egentligen är en mycket mer rättvisande beskrivning av vad det rör sig om, nämligen en teknik för distribuerade eller delade liggare. Alla som deltar i en blockkedja delar exakt samma liggare i realtid och kan därigenom uppnås en grundläggande konsensus om t.ex. vem som äger vad just nu och exakt vilka transaktioner som historiskt har lett till detta nuläge. Detta är annars ett problem med vanliga liggare; de är typiskt sett privata och det går inte utan vidare att vara säker på att informationen i den är korrekt, inte minst som många kan ha ett starkt intresse av att manipulera informationen i den (läs Enron m.fl.).

Genom att blockhain-teknologin är en distribuerad teknologi kan den komma att utmana en mängd olika affärsmodeller och institutioner. En bank fyller en funktion genom att den avlastar en mängd långivare och låntagare från nödvändigheten att hitta och förhandla om lånevillkor med varandra. Dessutom kan banken garantera att den äger de pengar den lånar ut, vilket kan vara svårt att lita på att en privatperson gör. Blockkedjan kan här lösa såväl informations- som tillitsproblemet så i teorin innebär tekniken att banker inte behövs. Och eftersom banker kan sägas utgöra det ekonomiska systemets hjärta – de tar emot och pumpa ut pengar – så räcker det nog med att säga att banker kanske inte behövs för att man ska förstå att blockchain har en otroligt revolutionerande potential.

Tre juridiska problemområden

Bland de juridiska frågor som aktualiseras av en blockkedja är det tre som framstår som mest viktiga, nämligen

1. Juridisk kontroll av blockkedjan och informationen i den.
2. Regelefterlevnad vid användningen av blockkedjan, samt
3. Kontrakt om och i blockkedjan.

Jag kommer här att i korthet behandla vart och ett av dessa områden.

Juridisk kontroll av blockkedjan och informationen i den

Det finns både publika och privata blockkedjor. Bitcoin är en publik blockkedja: den ägs inte av någon och i princip vem som helst kan ansluta till den. De flesta blockkedjor kommer dock sannolikt att vara privata. De kan då inrättas av ett företag som sedan låter andra ansluta till den. Eller så kan den inrättas av flera företag vilka kanske också är de enda deltagarna i blockkedjan.

Två grundläggande frågor i både publika och privata blockkedjor är för det första vem som äger själva blockkedjan och för det andra vem som äger informationen i blockkedjan. En blockkedja är en distribuerad databas och lär oftast uppfylla

definitionen i artikel 1.2 i direktiv 96/9/EG av om rättsligt skydd för databaser. En databas definieras där som en samling av verk, data eller andra självständiga element som sammanställts på ett systematiskt och metodiskt sätt och som var för sig är tillgänglig genom elektroniska medier eller på något annat sätt. Men en blockkedja är en också slags mjukvara och skulle därför kunna omfattas av direktiv 91/250/EEG om rättsligt skydd för datorprogram. I båda fallen har upphovsmannen skydd men det är inte helt säkert vilken som är den korrekta upphovsrättsliga klassificeringen av blockkedjan.

När det gäller informationen *i* blockkedjan är saken än mer oklar. Det saknas regler om äganderätt till data. Det närmsta man kommer äganderätt är det s.k. sui generis-skyddet i databasdirektivet. En upphovsman kan, enligt artikel 7.2 i databasdirektivet, erhålla ett visst skydd för innehållet i en databas om denne har gjort en väsentlig investering vid anskaffning, granskning eller presentation av databasens innehåll. Det följer dock av praxis från EU-domstolen att de resurser som läggs ned på att skapa de element som utgör innehållet i en databas inte ska räknas in i denna investering. Eftersom en blockkedja utgör ett resultat av historiska transaktioner och inte av en aktiv anskaffning är det mer än osäkert om innehållet i blockkedjan åtnjuter sui generis-skydd. Möjligen skulle kunna hävdas att en väsentlig investering har gjorts för att granska informationen, eftersom det ingår i blockkedjans natur att verifiera informationens korrekhet.

I avsaknad av sui generis-skydd eller annat upphovsrättsligt skydd återstår egentligen endast skydd som företagshemlighet som möjlighet. Men för att information ska åtnjuta skydd enligt lagen om företagshemligheter ska den definitionsmässigt hållas hemlig. Det ligger dock i blockkedjans natur att den ska vara mer eller mindre publik för deltagarna i blockkedjan, varför det kan hävdas att informationen inte är skyddad.

Ovan har jag förstås endast gjort en endast grundläggande analys och det går inte att här uttala sig generellt om blockkedjor eller informationen i dem åtnjuter upphovsrättsligt eller annat skydd. Analysen ovan visar dock att saken ingalunda är självklar, vilket gör att det förstås är avgörande för företag som bildar blockkedjor att vidta åtgärder för att tillse det skydd som behövs.

Regelefterlevnad vid användning av blockkedjan

Ett annat viktigt område när det gäller blockkedjor är allmän regelefterlevnad. Än så länge saknas blockchain-specifika lagregler. Men det finns flera allmänna regelverk som, beroende på användningsområde, behöver beaktas när en blockkedja sätts upp och används. Konsumenträttslig lagstiftning och finansregulatorisk lagstiftning är två exempel. Det för tillfället kanske mest intressanta regelverket att titta på i dessa GDPR-tider är just GDPR så jag koncentrerar mig här på ett antal frågeställningar enligt detta regelverk.

En första frågeställningen rör då frågan om rollerna som personuppgiftsansvarig och personuppgiftsbiträde. Den är personuppgiftsansvarig som bestämmer ändamål och medel med behandlingen av personuppgifterna. Den är personuppgiftsbiträde som behandlar personuppgifter på uppdrag av den personuppgiftsansvarige.

Det ligger i blockkedjans natur att den är delad av flera. Det ligger därför nära tillhands att dra slutsatsen att alla eller åtminstone flera deltagare i blockkedjan ska anses vara personuppgiftsansvariga. Om det rör sig om en privat blockkedja upprättad av ett konsortium, vilket inte är ovanligt, rör det sig sannolikt om ett gemensamt personuppgiftsansvar. Det följer då av artikel 26 i GDPR att de gemensamt personuppgiftsansvariga under öppna former ska fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt förordningen. Detta behöver då fastställas i konsortialavtalet.

Detta förefaller okomplicerat. Mer komplicerat är då hur informationskraven i artiklarna 13 och 14 ska uppfyllas. De registrerade har rätt att känna till vem eller vilka som är personuppgiftsansvariga och därför behöver information lämnas om alla personuppgiftsansvariga i blockkedjan.

Även detta går att lösa. Det blir svårare när det kommer till de registrerades rättigheter enligt artikel 16 att få felaktig information rättad och enligt artikel 17 att få sina personuppgifter raderade (rätten att bli glömd). Det ligger i blockkedjans grundidé att den inte ska kunna ändras i efterhand för om någon försöker göra det så bryts kedjan. Det ligger ännu mer i grundidén att informationen *inte* ska kunna raderas eftersom blockkedjan ska utgöra en transparent redogörelse över alla händelser som har lett fram till kedjans nuvarande status avseende äganderätt, kontroll eller vad dess liggare nu utvisar. Detta kan utgöra ett fundamentalt problem. Enligt artikel 25 i GDPR måste system uppfylla krav på inbyggt dataskydd, d.v.s. de måste vara designade för att möjliggöra en korrekt behandling av personuppgifter. Att bygga en blockkedja utan förutsättningar för radering av uppgifter som inte längre får behandlas är därför olagligt från och med den 25 maj 2018.

Kontrakt i och om blockkedjan

Många juristers intresse för blockkedjor väcks genom begreppet ”smarta kontrakt”. Vilket är lite lustigt eftersom ett smart kontrakt egentligen inte är ett kontrakt alls i juridisk mening. Ett smart kontrakt är istället en mjukvarukomponent i blockkedjan som utför vissa kommandon om den blir anropad på rätt sätt. Men ofta innebär dessa

kommandon att transaktioner utförs – exempelvis kan pengar eller äganderätter förflyttas – så det blir ändå inte onaturligt att här tala om kontrakt även i juridisk bemärkelse.

Det finns ett antal juridiska delfrågor som aktualiseras av smarta kontrakt. Än så länge verkar de dock inte vara speciellt intressanta, åtminstone inte i mitt personliga tycke.

Då framstår kontrakten *om* blockkedjan som betydligt intressantare. Det går här att göra skillnad på ett anta olika typer av kontrakt. En första kontraktstyp utgörs av ett vanligt tjänstekontrakt genom vilket en leverantör tillhandahåller en tjänst baserad på blockkedjeteknik. Sådana tjänster blir och kommer att bli allt vanligare. I många fall handlar det då inte om något mer komplicerat än ett molntjänstavtal där emellertid de ovan nämnda utmaningarna enligt dataskyddslagstiftningen behöver hanteras.

En andra kontraktstyp utgörs istället av ett samarbetsavtal eller motsvarande där ett antal aktörer avtalar om att bilda och verka i en blockkedja tillsammans. Denna typ av kontrakt kan utgöra en riktig utmaning. Som teknik löser blockkedjan ett transparens- och tillitsproblem. Men blockkedjetekniken kan inte lösa de utmaningar som uppstår när avtalet *om* en specifik blockkedja ska ingås. För att en blockkedja ska bli framgångsrik måste alla som ansluter till den kunna lita på att informationen i den distribuerade liggaren är korrekt. Detta förutsätter att ingen kan misstänka att informationen har blivit manipulerad, vilket i sin tur innebär att det är viktigt att se till att ingen får för stor makt över blockkedjan. Alla som bildar eller ansluter till en blockkedja måste på någon nivå få samstämmiga intressen i att upprätthålla blockkedjans integritet.

I publika blockkedjor som Bitcoin och Etherum har man försökt lösa detta problem på ett briljant sätt. Med viss frekvens skapas nya block, som registrerar den senaste periodens transaktioner i blockkedjan, vilka genom hashning länkas tillbaks till tidigare block för att garantera en obruten kedja. Om det var en och samma aktör som alltid skapade dessa block skulle ett tillitsproblem till informationens korrekthet definitivt kunna uppkomma. Bitcoin och Etherum är därför riggade som spel, där s.k. miners, kämpar om att få vara den som skapar nästa block genom att lösa ett svårt matematiskt problem. Belöningen är – förstås – bitcoins eller ether. På detta sätt blir det mycket slumpen som avgör vem som skapar nästa block och alla miners har ett intresse av att bibehålla blockkedjans integritet eftersom deras intjänade valuta annars riskerar att förlora i värde. Gamla Adam Smith måste vara lycklig i sin himmel när han ser detta sätt att få alla att bidra till det gemensamma bästa genom att tänka på sig själva.

De som tillsammans ska upprätta en privat blockkedja behöver i princip lösa samma problem, men utan blockkedjans hjälp. De behöver skapa ett samarbete som håller deras intressen samstämmiga. Detta innebär en utmaning eftersom de flesta kontrakt som skrivs inte skrivs för att skapa samstämmiga intressen utan primärt för att skydda sig mot de motstridiga intressen som man antar att man har eller kommer att få. Därför anser jag att denna typ av samarbeten behöver inrättas på basis av s.k. relationsbaserade kontrakt, som syftar just till att skapa kontinuerligt samstämmiga intressen mellan parterna.

Avslutning

Det finns ingen blockchain-juridik. Som alltid springer teknikutvecklingen snabbare än rättsreglerna och regler utvecklade på ett tidigare utvecklingsstadium måste fortsätta att tillämpas. De bristfälliga reglerna rörande ägande och kontroll av information och data kan ofta lösas med kontrakt. Spänningsförhållandet mellan blockkedjetekniken och personuppgiftslagstiftningen verkar då svårare att hantera. Samtidigt är det problemet i huvudsak just tekniskt och har mänskligheten nått så långt att man har kommit på blockchain-tekniken ska man nog kunna lösa det problemet också.

David Frydlinger är delägare och advokat i Advokatfirman Lindahl, Stockholm.

Nu regleras artificiell intelligens på allvar ur ett dataskyddsperspektiv

av Linus Larsén,
Advokatfirman Delphi.

Inledning

Nya tekniska innovationer baserade på mer eller mindre självlärande system som går under benämningen artificiell intelligens (AI) blir allt vanligare. Tekniken brukar beskrivas som intelligenta system som utför uppgifter som traditionellt har utförts av människor. De senaste åren har noterbara framsteg avseende tekniken gjorts bland annat vad gäller självkörande bilar, bild- och röstigenkänning och smarta assistenter, som Amazons Alexa och Apples Siri. Inom den privata sektorn har bland annat banker och försäkringsbolag tidigt intresserat sig för den nya tekniken och de möjligheter som en utökad automation medför. Även det offentliga har intresserat sig för användandet av AI, bland annat inom myndighetsutövning. Nyligen har det till exempel uppmärksammats att flera kommuner i Sverige börjat använda automatiska handläggningssystem för att avgöra om ansökningar ger rätt till försörjningsstöd eller inte.[1] Liknande beslutsstöd tillämpas redan eller har föreslagits på många andra områden inom den offentliga sektorn.

Linus Larsén

Användandet av AI-teknik kan ha många fördelar, exempelvis ökad effektivitet och minskad risk för handläggningsfel som beror på mänskliga misstag. Samtidigt kan användandet av AI för att fatta beslut som påverkar individer vara både integritetskänsligt och potentiellt leda till transparensproblematik. Risken finns också att mänskliga snedvridningar och fördomar vid beslutsfattande återskapas i de automatiska beslutsprocesserna, som i ett exempel från USA där ett system som använts för att för att avgöra sannolikheten för framtida brottslighet anklagats för att diskriminera människor utifrån hudfärg.[2] Avvägningar mellan fördelarna och nackdelarna med AI gör att frågan om att reglera AI och automatiska beslut blivit alltmer angelägen.

Redan i det nu gällande dataskyddsdirektivet från 1995 (direktiv 95/46/EG) och den på direktivet baserade svenska personuppgiftslagen finns en bestämmelse om automatiska beslut. Bestämmelsen, artikel 15 i direktivet som fått en begränsad praktisk betydelse, tillåter generellt sett automatiska beslut samtidigt som vissa grundläggande rättigheter för den registrerade garanteras. I bestämmelsens första stycke ges personer som omfattas av ett automatiskt beslut rätt att begära en mänsklig omprövning av beslutet, förutsatt att detta är avsett att bedöma egenskaper hos den berörda personen, samtidigt som beslutet har rättsliga följder eller andra märkbara verkningar för personen i fråga. Genom stycke två ges den registrerade också en rätt att ansöka om att få information om vilka orsaker som legat bakom det automatiska beslutet.

I den nya dataskyddsförordningen (GDPR) har bestämmelsen om automatiskt beslutsfattande från det tidigare direktivet uppdaterats, med förordningens artikel 22 som den centrala bestämmelsen. Även andra bestämmelser i GDPR kan få betydelse för beslut som fattas med hjälp av AI. Artikel 29-gruppen publicerade i oktober 2017 en ny vägledning om automatiskt beslutsfattande och

1 Dagens Nyheter, *Socialsekreterare slutar i protest när robot hanterar ansökningar,* 2018-01-21, https://www.dn.se/ekonomi/jobb-karriar/socialsekreterare-slutar-i-protest-nar-robot-hanterar-ansokningar/1 & Robot ledde till färre bidragstagare, 2018-01-08, https://www.dn.se/nyheter/sverige/robot-ledde-till-farre-bidragstagare/.

2 ProPublica, Machine Bias, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

profilering som tolkar bestämmelsen i artikel 22 och andra anknytande bestämmelser i förordningen.[3]

Vad är profilering och automatiska beslut enligt GDPR?

Profilering är ett nytt begrepp som tillkommit i GDPR för vissa analyser och bedömningar av personer. Begreppet definieras i artikel 4.4 i GDPR som

> ”*varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar*”.

Enligt bestämmelsen måste profilering innehålla moment av automatisk behandling, behandlingen måste avse personuppgifter och även utvärdera en registrerad persons egenskaper. Ett typexempel på profilering är när uppgifter om andra personer i en i förväg definierad grupp bedöms på automatisk väg utifrån aspekter som kön, ålder och inkomst för att förutspå hur en registrerad ska agera i en viss situation. Den här typen av behandling är bland annat vanlig vid beteendebaserad reklam riktad mot vissa målgrupper och sådana komplexa analyser och datautvinning som sker i samband med *big data*.

Automatiska beslut kan baseras på profilering men behöver inte göra det. Artikel 29-gruppen definierar ett beslut som enbart grundas på automatiserad behandling som ett beslut som fattas på teknisk väg utan mänsklig inblandning.

Ett generellt förbud mot vissa automatiska beslut

Av artikel 22.1 i GDPR framgår att det som huvudregel är förbjudet med beslut som enbart grundar sig på automatiserad behandling och som inbegriper profilering, om beslutet har rättsliga eller andra märkbara konsekvenser för den registrerade. Bestämmelsen ställer alltså upp större begränsningar mot den här typen av automatiska beslut än vad som är fallet enligt personuppgiftslagen i nuläget. Att ett beslut ”enbart” baserar sig på automatiserad behandling innebär som beskrivits ovan enligt Artikel 29-gruppen att det saknas någon form av meningsfull mänsklig inblandning i beslutsfattandet, istället sker alla aspekter i en beslutfattningsprocess på automatisk väg. Det är enligt Artikel 29-gruppen inte möjligt att fingera mänsklig inblandning. Skulle en mänsklig handläggare godkänna ett beslut som föreslagits på helt automatisk väg utan att göra några egna reella överväganden eller ställningstaganden bör beslutet ändå ansetts fattats på enbart automatisk väg.

För att ett beslut ska omfattas av förbudet krävs också att det inbegriper profilering. Många svenska myndighetsbeslut som fattas på automatisk väg har tidigare ansetts falla utanför bestämmelsen om automatiskt beslutsfattande i personuppgiftslagen eftersom besluten inte ansetts bedöma människors beteenden på det sätt som nu kallas profilering enligt den nya definitionen i GDPR. Ett exempel som ges av Artikel 29-gruppen på när ett myndighetsbeslut kan innefatta profilering är utfärdandet av fortkörningsböter med hjälp av en hastighetskamera. Skulle ett beslut enbart grundas på en objektiv registrering av ett fordons hastighet är det inte fråga om profilering, då ingen bedömning av bilförarens personliga egenskaper sker. Skulle det däremot tas in andra aspekter för att bestämma bötesbeloppets storlek, såsom förarens generella körvanor och tidigare förseelser, blir det istället fråga om en sådan bedömning av personliga egenskaper som anses vara profilering enligt GDPR och artikel 22 kan bli tillämplig.

Slutligen måste beslutet i fråga också ha rättsliga följder eller påverka den registrerade ”*på ett liknande sätt i betydande grad*” för att omfattas av förbudet i artikel 22.1. Begreppet rättsliga följder definieras inte i GDPR men Artikel 29-gruppen ger i sin vägledning flera exempel på vad som enligt gruppens uppfattning kan utgöra rättsliga följder för en registrerad, i situationer när dennes rättigheter enligt lag eller avtal påverkas. Situationer där det är fråga om rättsliga följder är exempelvis att den registrerade nekas socialbidrag, vägras gränspassering, blir föremål för utökad övervakning av myndigheter eller blir frånkopplad från sitt telefonabonnemang på grund av en obetald telefonräkning. För att ett beslut ska anses påverka den registrerade på ”*ett liknande sätt i en betydande grad*”, som om ett beslut skulle haft rättsliga följder krävs enligt Artikel 29-gruppen att beslutet

---

3 Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation* 2016/679, antagen den 3 oktober 2017, *http://ec.europa.eu/newsroom/document.cfm?doc_id=47742*. Se vidare även norska Datatilsynet och brittiska ICOs rapporter om Artificiell Intelligens och dataskydd: Datatilsynet, Kunstig intelligens og personvern, januari 2018, *https://www.datatilsynet.no/om-personvern/rapporter-og-utredninger/kunstig-intelligens/* samt ICO, Big data, artificial intelligence, machine learning and data protection, september 2017, https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/.

har en viss nivå av betydelse för den registrerade och påverka dennes beteende, beslut eller omständigheter i övrigt. Exempel ges i beaktandeskäl 71 i GDPR som ”*automatiskt avslag på en kreditansökan online eller e-rekrytering utan personlig kontakt*”. Vad som kan utgöra beslut som påverkar registrerade utan att ha rättsliga följder kommer sannolikt att behöva förtydligas utöver de exempel som ges i beaktandeskälen.

Undantag från förbudet

Det finns tre huvudsakliga undantag från det generella förbudet mot automatiskt beslutsfattande enligt artikel 22.1. Dessa är (i) om behandlingen är nödvändig för en avtalsförbindelse mellan den registrerade och den personuppgiftsansvarige, (ii) om beslutet är tillåtet enligt EU-rätten eller nationell rätt samt (iii) om den registrerade har lämnat sitt uttryckliga samtycke till behandlingen. Nödvändigheten för att fullgöra en avtalsförbindelse anknyter till den motsvarande rättsliga grunden i artikel 6.1 b) i GDPR. Värt att notera är att nödvändighetskravet ska tolkas snävt vilket gör att den här rättsliga grunden inte alltid är lämplig när nödvändigheten av behandlingen kan ifrågasättas.

Rättsligt stöd kan också finnas i nationell lagstiftning eller i EU-rätt. Ett begränsat antal bestämmelser som uttryckligen tillåter automatiserade beslut finns avseende myndigheter och förvaltningen i Sverige. Noterbart är att det i det svenska betänkandet *SOU 2014:75 Automatiserade beslut – färre regler ger tydligare reglering* (som presenterades innan GDPR färdigställdes), drogs slutsatsen att automatiska beslut inom myndigheters verksamhet generellt inte kräver lagstöd och att nya sådana bestämmelser inte bör införas i svensk rätt. I och med den nya bestämmelsen i artikel 22 i GDPR och myndigheters ökade intresse för att använda allt mer sofistikerad teknik för automatiskt beslutsfattande blir frågan på nytt aktuell och vissa av slutsatserna i den tidigare utredningen kan behöva omvärderas. För att detta undantag ska kunna bli aktuellt krävs att det rättsliga stödet för besluten också garanterar den registrerade vissa grundläggande rättigheter och säkerheter, något som idag sker i personuppgiftslagen genom möjligheterna att bestrida ett beslut och få information om beslutsprocessen.

> Meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling av sådan behandling för den registrerade

Det tredje undantaget från förbudet mot automatiska beslut enligt artikel 22, *uttryckligt samtycke*, innebär att högre krav ställs för att inhämta ett samtycke än det generella kravet i GDPR. Samma krav ställs enligt förordningen för att behandla särskilt känsliga personuppgifter med stöd av ett samtycke enligt artikel 9.2 a). I Artikel 29-gruppens nya vägledning om samtycke diskuteras vad kravet på uttryckligt samtycke ska anses innebära och det konstateras att ytterligare förtydliganden kan behöva göras.[4] Artikel 29-gruppen ger som exempel på uttryckliga samtycken tydliga bekräftelser på samtycken i skrift, genom elektronisk legitimering eller tvåstegsautentisering.

För att automatiska beslut enligt artikel 22 som innefattar behandling av särskilt känsliga personuppgifter ska få fattas ställs särskilda krav. Enligt artikel 22.4 krävs det antingen uttryckligt samtycke till behandlingen eller att artikel 9.2 g) är aktuell, det vill säga att beslutet fattas med stöd av viktiga allmänna intressen, förankrade i EU-rätten eller nationell lagstiftning. Den här bestämmelsen skulle gissningsvis kunna ha betydelse bland annat för användandet av AI-system för beslutsfattande i sjukvården vid diagnosställande och behandling av patienter, där profilering exempelvis kan användas för att bedöma sannolikheten för att en patient drabbas av en sjukdom genom att analysera olika demografiska grupper.

Lämpliga säkerhetsåtgärder, informationskrav och övriga skyldigheter

Registrerade som omfattas av automatiserade beslut enligt artikel 22 är garanterade vissa skyddsåtgärder i enlighet med artikel 22.3. Bland den registrerades rättigheter ingår också rätten att bli informerad enligt artikel 13 och 14. Avseende automatiska beslut som omfattas av artikel 22 finns specifika informationskrav för personuppgiftsansvariga i artikel 13.2 f), 14.2 g) och 15.1 h). Bland annat ska information lämnas om att automatiskt beslutsfattande förekommer i den personuppgiftsansvariges verksamhet och ”*meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling av sådan behandling för den registrerade*”. Detta informationskrav kan skapa utmaningar vid vissa typer av beslut som fattas av mer komplexa AI-system, bland annat vid användandet artificiella neuronnät och djupinlärningsteknik som ökat i betydelse de senaste åren. I sådana system finns ofta en så kallad ”black box-problematik” där det kan vara svårt att avgöra hur systemens algoritmer fungerar och hur vissa typer av beslut fattas och därför gör det svårare att lämna tillfredsställande information till den registrerade.

Den registrerade har enligt artikel 22.3 även en rätt att göra invändningar mot ett beslut om det base-

4 Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation* 2016/679, antagen den 28 november 2017, s. 18 f., http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849.

rats på att det nödvändigt för att fullgöra en avtalsförbindelse eller om den registrerade gett sitt uttryckliga samtycke till behandlingen. Den registrerade ska bland annat få uttrycka sin åsikt och bestrida beslutet och har dessutom rätt till personlig kontakt med den personuppgiftsansvarige med anledning av beslutet. Exakt vilka konsekvenser som inträder genom bestridandet av ett beslut är något oklart. Det är tveksamt om det går att tolka formuleringen i förordningstexten så långt som en rättighet för den registrerade att alltid få överklaga och ompröva den här typen av beslut, även om rätten till överklagan nämns i beaktandeskäl 71 till förordningen. Skälen till förordningen är dock inte bindande. En rätt till mänsklig omprövning finns även i föregångsbestämmelsen i personuppgiftslagen. Artikel 29-gruppens bedömning är att rätten till personlig kontakt med den personuppgiftsansvarige innebär att en person hos den personuppgiftsansvarige som har behörighet att ändra ett beslut granskar all relevant data för beslutet, inklusive eventuella nya uppgifter från den registrerade. Formuleringen är problematisk med tanke på mängden data och aspekter som förekommer inom ramen för beslutsfattande i mer komplexa system. Ytterligare förtydliganden kring denna rätt till invändningar kommer sannolikt att behövas.

Vid användande av AI och automatiska beslut kan även andra bestämmelser i GDPR bli aktuella. Det finns exempelvis en skyldighet att göra en konsekvensbedömning (Data Protection Impact Assessment) när automatiskt beslutsfattande som inbegriper profilering används i stor utsträckning och hänsyn behöver även tas till de bestämmelser om inbyggt dataskydd för system som finns i förordningen (Privacy by design/default).

De grundläggande principerna för personuppgiftsbehandling i artikel 5 anses också kunna vara betydelsefulla i synen på hur AI-system lever upp till GDPRs integritetskrav. Dessa omfattar bland annat korrekthet, öppenhet, ändamålsbegränsning och uppgiftsminimering.

Praktiska konsekvenser

GDPR innebär nya praktiska konsekvenser av betydelse för de aktörer som använder AI på olika sätt, särskilt vid automatiskt beslutsfattande. Med anledning av de särskilda krav som ställs på vissa beslut enligt artikel 22 bör personuppgiftsansvariga som använder sig av automatiskt beslutsfattande analysera huruvida beslutsfattandet sker på ett sådant sätt att det omfattas av bestämmelsen. Skulle ett beslut omfattas av bestämmelsen blir det i nästa steg viktigt att identifiera en lämplig rättslig grund för behandlingen utifrån de alternativ som framgår av bestämmelsen. För privata aktörer bör denna grund normalt sett vara att fullgöra ett avtal eller att den registrerade lämnat sitt uttryckliga samtycke. Om offentliga aktörer har infört eller planerar att införa beslutssystem som innefattar profilering är det viktigt att inse vilka konsekvenser detta medför. De offentliga aktörerna kan i normalfallet inte lämpligen behandla uppgifter med stöd av ett avtal eller genom att inhämta samtycke. Det blir därför viktigt att analysera om behandlingen kan anses tillåten enligt lag. Den bedömning som gjordes i betänkandet SOU 2014:75 där automatiska beslut generellt setts ansetts tillåtna enligt svensk rätt kan sannolikt inte längre ges betydelse för beslut som omfattas av artikel 22 i GDPR. Av den anledningen har även lagstiftaren en väldigt viktig uppgift framför sig genom att vidare utreda vilken ny lagstiftning som behöver introduceras för att myndigheter ska kunna använda AI i sin verksamhet på ett lämpligt sätt.

Utmaningar väntar både privata och offentliga aktörer för att säkerställa registrerades rättigheter avseende information och möjligheten att ifrågasätta ett automatiskt beslut. Den personuppgiftsansvarige måste ta fram rutiner både för att hantera klagomål från enskilda avseende automatiska beslut men även för att lämna information avseende dessa beslut. Det behövs fortfarande förtydliganden om hur långtgående enskildas rättigheter är vad gäller möjligheterna att bestrida beslut som fattas på automatisk väg och det är oklart hur informationstexter ska kunna förklara ofta mycket komplexa tekniska beslutsprocesser på ett tillfredsställande sätt. Det blir viktigt att implementera rutiner som ser till så att AI-system utformas och utvecklas så att data behandlas på ett begränsat, transparent och säkert sätt. Vi har bara sett början på diskussionen om dessa allt mer betydelsefulla frågeställningar om dataskydd och AI som aktualiseras. Aktörer som misslyckas med att följa GDPRs krav vid utformningen och användningen av AI-system riskerar skarpa sanktionsavgifter enligt förordningen. Nu regleras AI på allvar ur ett dataskyddsperspektiv.

Linus Larsén är associate i Advokatfirman Delphi, Stockholm.

Innovative IT-anskaffelser

av Espen Bakjord og
Marianne H. Dragsten,
Synch Advokatfirma AS.

Espen Bakjord

Marianne Dragsten

Det å foreta innovative anskaffelsesprosesser er i vinden. Vi antar at mange oppdragsgivere ønsker seg nettopp en slik anskaffelsesprosess. Men hva er egentlig innovative anskaffelser? Og hvis det er uklart hva en innovativ anskaffelse er, gir det mening å snakke om innovative *IT-anskaffelser*?

For den som tidligere har satt seg inn i temaet, kan terminologien i denne artikkelen oppfattes noe anakronistisk. Før omtalte man gjerne innovative anskaffelser som «innovative teknologiske anskaffelser», eller public technology procurement (PTP).[1] Dette uttrykket har man nå forlatt, kanskje med tanke på at innovasjon handler om mer enn bare teknologi. Når vi i denne sammenheng likevel fremhever IT-anskaffelser som noe av det viktigste på dette området, kan det hevdes at ringen er sluttet.

Offentlige anskaffelser ser ut til å bli et stadig viktigere strategisk virkemiddel for å stimulere til innovasjon. Når ulike oppdragsgivere legger opp til og gjennomfører innovative anskaffelser, utøves det en dra-kraft i markedet etter innovative varer og tjenester.

Her kan det også vises til Produktivitetskommisjonens andre rapport NOU 2016:3 *Ved et vendepunkt: Fra ressursøkonomi til kunnskapsøkonomi*. I rapporten analyseres blant annet mulighetene for å hente ut mulige innovasjonsgevinster i anskaffelsesprosessene. En av konklusjonene ser ut til å være at innovasjon i offentlig sektor er vanskelig uten en vesentlig liberalisering av anskaffelsesregelverket.[2]

Hva er en innovativ anskaffelse?

Leser vi Difis presentasjon av temaet på deres nettsider, er innovative anskaffelser «et utvalg av metoder og verktøy for å få bedre behovsdekning i en anskaffelse». Videre heter det at anskaffelsesprosessene må åpne for nyskapning. Direktoratet fremhever også at det som etterspørres i anskaffelsen bør være en vare eller en tjeneste som på en eller flere måter innebærer noe nytt, eller som representerer en optimalisering eller videreutvikling av noe som finnes i dag.[3]

Spørsmålet er om denne beskrivelsen er så vid at det blir vanskelig å få øye på hva som skal til for at en anskaffelsesprosess skal kunne kalles innovativ. Videre kan det spørres om ikke en innovativ anskaffelse bør resultere i at det utvikles noe nytt, som helst også tas i bruk. Bør det først og fremst fokuseres på metodene i anskaffelsesprosessene, eller på resultatet? Her kan det vises til anskaffelsesforskriften § 4-5 bokstav h, der innovasjon er definert på følgende vis:

> *innføring av en ny eller betydelig forbedret vare, tjeneste eller prosess, inkludert produksjons-, bygge- eller anleggsprosesser, en ny markedsføringsmetode eller en ny organisasjonsmetode innen forretningspraksis, arbeidsplassorganisering eller eksterne relasjoner.*

Nasjonalt program for leverandørutvikling

Difi, KS og NHO har gått sammen om et eget Nasjonalt program for leverandørutvikling,[4] der innovative anskaffelser står sentralt.[5] Programmet har hatt ganske stor suksess.

På oppdrag fra leverandørutviklingsprogrammet la Menon Economics i september 2017 frem en

1 Se eksempelvis *Public technology procurement and innovation* ved Edquist, Hommen og Tsipouri (Linköping/Athen 1999).

2 Det vises her til pkt 7.8.5: «Kommisjonen mener det bør være færrest mulig andre mål enn effektiv ressursbruk. Ethvert nytt mål vil kunne svekke konkurransen, fordyre offentlige innkjøp og komplisere regelverket.»

3 Se Difis nettsider for en utfyllende liste og beskrivelse: *https://www.anskaffelser.no/innovasjon/hva-er-innovative-anskaffelser*

4 Leverandørprogrammet ble startet i 2010. Se anskaffelser.no og innovativeanskaffelser.no.

5 Begrepet innovative anskaffelser er etter det vi kan se ikke nærmere definert, men det er uttalt at innovative anskaffelser innebærer å gå i dialog med markedet før anskaffelsen, formidle behovet og overlate løsningen til leverandørene.

midtveisrapport[6] som viste at det i 2010 bare var foretatt 6 innovative anskaffelser, mens i 2016 var foretatt ca. 180. Andelen innovative anskaffelser utgjør nå 1,4 prosent av antallet anskaffelsesprosesser. Nærmere 70 prosent av de innovative anskaffelsene som har blitt gjennomført mens leverandørutviklingsprogrammet har vart, skal ha fått bistand fra programmet.

Slik vi forstår rapporten side 7, er den anvendte definisjonen av en innovativ anskaffelse først og fremst knyttet til hvorvidt oppdragsgiver har involvert markedet og/eller leverandørene i form av et dialogmøte/konferanse/seminar eller lignende.

Hva sier EU

EUs Horisont 2020-program er etter vår oppfatning et egnet utgangspunkt når det gjelder definisjoner av innovative anskaffelser. Blant de mest aktuelle definisjoner er de såkalte PCP- og PPI-prosesser.

PCP (Pre-commercial procurements), oversettes gjerne med førkommersielle anskaffelser. Disse prosessene omfatter normalt forsknings- og utviklingstjenester (FoU). PCP er likevel ikke det samme som inngåelse av en FoU-kontrakt i forskriftens eller anskaffelsesdirektivets forstand. PCP-anskaffelser er unntatt anskaffelsesdirektivene.[7]

PPI (Public procurement of innovative solutions) er anskaffelser av innovative varer eller tjenester. Det er hovedsakelig PPI-prosessene som omtales nærmere i denne artikkelen. Dette er anskaffelsesprosesser som følger reglene i anskaffelsesdirektivet. PPI-definisjonen i Horisont 2020-programmet er som følger:

Behovs- og markedsundersøkelser			
Behov for FoU?			
JA		NEI	
Skal det anskaffes innovative produkter som en del av anskaffelsesprosedyren?		Har man tilstrekkelig grunnlag til å utforme kravspesifikasjon?	
JA	NEI	NEI	JA
Innovasjons-partnerskap	«Før-kommersielle anskaffelser» (PCP)	Konkurransepreget dialog (PPI)	Konkurranse med forhandling (PPI)

> *'Public procurement of innovative solutions (PPI)' means procurement where contracting authorities act as a launch customer of innovative goods or services which are not yet available on a large-scale commercial basis, and may include conformance testing.*

Slik vi oppfatter det, er dette en mer fremoverlent definisjon enn den vi omtaler ovenfor.

Nå kan det innvendes at det ikke er et stort problem om resultatet er innovasjon eller ikke, så lenge oppdragsgiverne trekker i en mer innovativ retning og åpner for at innovasjon kan skje. Slike prosesser må uansett regnes for å være et langt skritt i riktig retning sammenlignet med tradisjonell gjennomføring.

Ut fra denne betraktningen synes det fornuftig at en innovativ anskaffelsesprosess kjennetegnes av en inngående behovsvurdering og ved at det foretas leverandørdialog i tidlig fase av anskaffelsesprosessen. I tillegg kan man trekke frem samspillet mellom innkjøpere og etterfølgende evaluering og erfaringsutveksling.

For oversiktens skyld har laget følgende tabell, som viser de mest sentrale variantene av de ulike innovative anskaffelsesprosessene.

Nærmere om innovative IT-anskaffelser

Etter vår vurdering står vi overfor en innovativ IT-anskaffelse når IT-løsningen utgjør anskaffelsens hovedytelse. Innovative anskaffelser som eksempelvis gjelder bedre klimastyring, energioptimalisering, og vesentlig forenklede produksjons- eller byggeprosesser er klart nok viktige og interessante områder, og som gjerne kan ha en klar IT-teknisk side. Denne type anskaffelser er likevel ikke alltid innovative *IT-anskaffelser.*

Likevel, selv om man legger EUs nomenklaturregler til grunn, kan grensen mellom en innovativ anskaffelse og en innovativ IT-anskaffelse oppleves flytende. Det kan derfor være en smakssak om man ønsker å foreta denne type inndelinger av innovative anskaffelser, der det skilles mellom hvilke typer varer og tjenester som etterspørres. I det følgende presenteres noen analyser og praktiske erfaringer med IT-anskaffelser i PPI-sammenheng, særlig med tanke på prosedyren konkurranse med forhandling.

Grundig behovsvurdering – mindre detaljerte kravspesifikasjoner

En behovsvurdering og etterfølgende kravspesifisering i forbindelse med IT-anskaffelse er ofte en omfattende og komplisert øvelse. Det har eksempelvis blitt forsket på hvordan man skal angi en presis kravspesifikasjon som leder frem til det systemet man vil ha, samtidig med at anskaffelsesregelverket ivaretas.[8] Det kreves også en høy grad

6 Midtveisevaluering av nasjonalt program for leverandørutvikling (Menon-publikasjon nr. 55/2017).

7 Se anskaffelsesdirektivet artikkel 14, forsyningsdirektivet artikkel 32 og forsvars- og sikkerhetsdirektivet artikkel 13 (f)(j).

8 Se for eksempel *The public procurement of information systems: dialectics in requirements specification,* ved C. E. Moe, M. Newman og M. K. Sein, European Journal of Information Systems (2017).

av interaksjon mellom leverandør og oppdragsgiver for at man skal kunne komme frem til den beste IT-løsningen. Anskaffelsesregelverket blir gjerne trukket frem som et hinder i så måte.

I en innovativ IT-anskaffelse kommer de tradisjonelle utfordringene enda mer på spissen. Spørsmålet bør ikke være hvordan man skal detaljspesifisere det man har, og heller ikke hvordan man skal detaljspesifisere det man ønsker seg. Etter vår oppfatning, og særlig når det gjelder innovative anskaffelser, mener vi det vil være mer hensiktsmessig å definere behovet uten at man går veien om en detaljspesifikasjon. På denne måten skaper man rom for at leverandørene gir tilbud på de gode og innovative løsningene som dekker oppdragsgivers behov.

Dette innebærer også å gi slipp på tanken om de unike skreddersydde IT-systemer. Fra tid til annen kan dette kanskje oppleves umulig, enten på grunn av innlåsningseffekter[9] eller at systemet løser en oppgave som ikke er relevant for andre og som heller ikke ligner på noe annet. I den utstrekning detaljkravene ikke kan forlates, vil det antakelig også være krevende å gjennomføre en innovativ anskaffelse, og ikke minst vanskelig å legge til rette for innovasjon.

Planlegging, dialog og markedsundersøkelser

Det er i planleggingsfasen av anskaffelsen at rammene for anskaffelsen, og dermed også mulighetsrommet for innovasjon, fastsettes. Oppdragsgiver må derfor i denne fasen ha fokus på hvorvidt og på hvilken måte innovasjon er ønskelig.

Det er dermed avgjørende at oppdragsgiver i denne fasen har tid til å gjennomføre nødvendige undersøkelser internt i egen organisasjon, samt at man kontakter andre oppdragsgivere som har gitt seg i kast med tilsvarende utfordringer, eller kanskje til og med løst tilsvarende behov. Videre bør det foretas dialog med brukerne om behovet og innhentes informasjon fra leverandørene om mulighetsrommet.

Skal anskaffelsen munne ut i innovasjon, vil vi si at en nødvendig forutsetning for dette er at oppdragsgiver har kontakt med leverandørmarkedet allerede i planleggingsfasen. Hvordan dette gjøres er opp til oppdragsgiver og det er mange måter å gjøre det på. En fremgangsmåte vi har sett at er effektiv, er at oppdragsgiver når behovsavklaringen har kommet tilstrekkelig langt, sender kravspesifikasjonen/konkurransegrunnlaget ut «på høring» slik at aktuelle leverandører kan komme med innspill til hvordan innovasjon kan ivaretas i prosessen/anskaffelsen.

For å nå ut til mange leverandører, herunder leverandører man ikke kjenner til, er det å anbefale at en slik «høring» kunngjøres ved bruk av en veiledende kunngjøring i DOFFIN/TED. En slik høring kan gjerne etterfølges av én-til-én møter med de leverandørene som har gitt de mest lovende innspillene. Det er ikke noe i veien for at oppdragsgiver har egne møter med enkeltleverandører. Kravet til likebehandling i anskaffelsesloven § 4 stenger ikke for det. I tillegg, og særlig ved en innovativ anskaffelse, vil det også være relevant å aktivt sondere terrenget for mulige leverandører da ikke alle aktuelle leverandører nødvendigvis følger med på kunngjøringene som legges ut på DOFFIN. Oppdragsgiver bør derfor også vurdereandre kanaler enn kunngjøringsdatabasen for å nå mulige leverandører, for eksempel å benytte sosiale medier.

Dialogprosessen foregår før selve den formelle anskaffelsesprosedyren settes ut i livet (altså før selve konkurransen kunngjøres) og er frivillig og uforpliktende både for leverandøren og for oppdragsgiver.

Etter vår erfaring er mange oppdragsgivere for tilbakeholdne med å ta kontakt med leverandørene, antakelig fordi man er redd for at en kontakt med leverandørene vil være i strid med kravet til likebehandling. I gjeldende anskaffelsesforskriften er det tydeliggjort at oppdragsgiver kan innhente råd fra leverandørene og ha dialog med markedet.[10] Dette fører forhåpentligvis til at flere oppdragsgivere tør å ha en aktiv dialog med leverandørmarkedet i forkant av anskaffelsen. Det er viktig å merke seg at forskriften som utgangspunkt ikke legger noen begrensninger på hvilken kontakt oppdragsgiver kan ha med leverandørene. Begrensningene ligger i hvordan rådene som leverandørene gir, brukes av oppdragsgiver. Rådene kan benyttes i planleggingen og gjennomføringen av anskaffelsen så lenge rådene ikke har konkurransevridende effekt eller fører til brudd på kravet til likebehandling. Oppdragsgiver har videre plikt til å sørge for å iverksette tiltak for å unngå at leverandørene ikke får en urimelig konkurransefordel. Reglene gir dermed mulighet for en god dialogprosess med leverandørmarkedet i planleggingsfasen.

Kvalifikasjonskrav og tildelingskriterier som premierer nytenking

Dersom målet er å oppnå gode innovative anskaffelser, må konkurransen legges opp slik at de leverandørene som presumptivt er innovative slipper inn i konkurransen. Det gjør at oppdragsgiver bør være kritisk og gjerne tenke annerledes enn tradisjonelt, når kvalifikasjonskravene,

9 Enkelte mener imidlertid at en innlåsning kan være bra i et innovasjonsperspektiv. Det vises eksempelvis til foredrag ved Jakobsen og Hvidsten på Dataforeningens IT-kontraktsdag 5. september 2017.

10 Se forskriften §§ 8-1 og 8-2 (forskriftens del II), og §§ 12-1 og 12-2 (forskriftens del III).

det vil si minstekravene for å kunne delta i konkurransen, fastsettes. Oppdragsgiver bør ikke fastsette flere kvalifikasjonskrav enn nødvendig og bør også ikke formulere kvalifikasjonskravene slik at de stenger for deltakelse fra nyetablerte virksomheter. Dette fordi det ofte kan være nyetablert firmaer som kan tilby de mest nyskapende tjenestene og disse firmaene vil kunne ha problemer med å møte en del av de «tradisjonelle» kvalifikasjonskravene som stilles av oppdragsgiverne.

Anskaffelsesforskriften åpner opp for at det kan benyttes tildelingskriterier som ivaretar livssykluskostnader. Selv om nye tjenester gjerne har en større oppstartskostnad, kan korrekt utformede tildelingskriterier som ivaretar livssykluskostnadene[11] være godt egnet til å sørge for at tilbydere som tilbyr innovative tjenester har mulighet for å vinne frem i konkurransen. Fokuseres det derimot kun på innkjøpspris kan det være vanskeligere å legge til rette for dette.

Oppdragsgiver bør også vurdere å benytte tildelingskriterier som premierer innovasjon. Tildelingskriterier som for eksempel «tilbudt grad av innovasjon», bør derfor vurderes. Det kan også være riktig å fokusere på leverandørens/tilbudts personells evne til å finne innovative løsninger. Det kan være krevende å lese ut av et tilbud hvordan den innovative graden av en tjeneste vil være. I en IT-anskaffelse kan det derfor være aktuelt å la tilbudt personell stille på intervju for å avdekke graden av innovasjon i den tilbudte prosessen.

Kort om mulige kontraktstyper

I forbindelse med innovative IT-anskaffelser vil særlig utviklingskontrakter være aktuelle verktøy. De gjeldende IT-utviklingskontrakter på markedet i dag forutsetter alle en høy grad av samspill mellom kunde og leverandør.

Relevante kontrakter i en innovativ IT-anskaffelse vil typisk være SSA-T (Utviklings- og tilpasningsavtalen), SSA-S (Smidigavtalen) og Dataforeningens PS 2000 Standard/Smidig og PS 2000 SOL. Dataforeningens skytjenesteavtale kan også vurderes, selv om denne ikke er en typisk IT-utviklingskontrakt.

Dersom oppdragsgiver selv ønsker å ha tilnærmet full kontroll med utviklingen av den innovative løsningen, kan oppdragsgiver vurdere rammeavtaler med bruk av avropsavtalene SSA-B og/eller SSA-O. I en slik gjennomføringsmodell vil det være oppdragsgiver som bestemmer hvordan den innovative tjenesten skal utvikles, og særlig hvis det bare etterspørres bistand (SSA-B). Dette er i så fall en annen tilnærming til innovative anskaffelser enn det som fremgår av definisjonen ovenfor.

Vi vil presisere her at det er planleggings- og behovsvurderingen som bør være styrende for hvilken kontrakt som velges, og ikke omvendt.

Risiko og risikoaversjon

Hva innebærer mest risiko – å sikte seg inn mot det sikre og velprøvde, eller å være innovativ? Litt forenklet synes det lite hensiktsmessig å foreslå «en gyllen middelvei» der oppdragsgiver legger opp til å være litt innovativ, i alle fall med tanke på hvilke løsninger det åpnes for. Når det gjelder økonomi må det offentlige klart nok forholde seg til gjeldende rammer. I noen tilfeller kan det også oppleves som uhensiktsmessig om det offentlige innlater seg på utvikling av mange løsninger på det samme problemet, selv om det er snakk om innovative prosesser som i seg selv har positive effekter på samfunnet.

I denne sammenheng er det interessant å peke kritikken mot utviklingen av to parallelle pålogingssystemer for det offentlige i Storbritannia. Her blir det trukket frem at de to systemene er en konsekvens av manglende kommunikasjon mellom offentlige organer, og at to systemer er sløsing av det offentliges midler.[12]

Her hjemme kan det vises til Digitaliseringsrundskrivet.[13] I 2017-utgaven er statlige virksomheter instruert om å ta i bruk ID-porten for «digitale tjenester som krever innlogging og autentisering». Det finnes også et knippe andre nasjonale fellesløsninger.[14] I alle fall fra et norsk perspektiv kan det derfor hevdes at man har funnet en rimelig balanse mellom fellesløsninger som bør etableres, og områder som bør utfordres og utforskes videre, og gjerne ved bruk av innovative anskaffelsesprosesser.

Selv om Norge i EU-sammenheng ligger godt an når det gjelder innovasjon, viser statistikken at de innovative anskaffelsene fortsatt er i et lite mindretall. Etter vår oppfatning har oppdragsgiverne fortsatt mye å gå på før frykten mot det ukjente bør sette inn.

Espen Bakjord er advokatfullmektig i Synch Advokatfirma AS.
Marianne H. Dragsten er advokat i Synch Advokatfirma AS.

11 Feks. ved bruk av det overordnede tildelingskriteriet beste forhold mellom kvalitet og kostnad.

12 Se *http://www.bestpracticegroup.com/bitter-turf-war-government-millions-spent-two-departments-potentially-duplicate-systems/*

13 Dette ble sendt ut første gang i 2009, den gang under navnet «Bedre planlegging og samordning av IKT-relaterte investeringer i staten».

14 Det vil si løsningene Digital postkasse, kontakt- og reservasjonsregisteret og eSignering, i tillegg til folkeregisteret, Brønnøysundregisteret og matrikkelen (Statens kartverk).

JusNytt

Halvor Manshaus

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

Hvor ble det av redaktørens erstatningsansvar for ærekrenkelser?

I norsk rett har vi i lang tid hatt et redaktøransvar. Dette ansvaret har tradisjonelt hatt tre sider, det strafferettslige ansvar, det erstatningsrettslige ansvar og det etiske ansvar. Gjennom innføringen av den nye straffeloven har vi i praksis mistet det erstatningsrettslige ansvaret for ærekrenkelser. Min påstand er at det per i dag ikke eksisterer noen lovhjemmel for å pålegge en redaktør et objektivt erstatningsrettslig ansvar for ærekrenkende innhold i en publikasjon.

Dette skjedde altså i forbindelse med ikrafttredelse av den nye straffeloven høsten 2015. Den nye loven gjennomførte en avkriminalisering av ærekrenkelser. Den gamle straffeloven inneholdt et eget kapittel 23 med egne bestemmelser om straffbare ærekrenkelser §§ 246 og 247, og en særregulering om mortifikasjon i § 253. Rettspraksis fra den Europeiske Menneskerettsdomstolen (EMD) som ble videreført av Høyesterett i blant annet saken Nordlandsposten (Rt-2002-764) medførte et paradigmeskifte der straffelovens bestemmelser ble satt til side og avløst av et stadig voksende knippe med rettsavgjørelser. Advokater som har jobbet på dette området har altså vært vant til å se bort fra straffelovens regulering av ærekrenkelser, og har i stedet fulgt domstolenes anvisninger på vurderingstemaene i konkrete saker. Rettskildebildet på dette området har altså vært sammensatt og vanskelig tilgjengelig for legfolk. Lovens ordlyd var ikke bare i utakt, men i direkte motstrid med gjeldende rett. Lovendringene i den nye straffeloven skulle fange opp disse endringene, slik at ærekrenkelsene forsvant ut av straffeloven og ble avkriminalisert. Mortifikasjonsinstituttet, der en ytring skulle kunne kjennes «død og maktesløs» ble også avviklet. I denne forbindelse ble også andre krenkelsesbestemmelser omregulert, blant annet ytringer knyttet til fremmed lands flagg og statsoverhoder.

Den gamle bestemmelsen om redaktøransvar i tidligere lovs § 431 ble videreført i ny § 269, og omhandler kun det strafferettslige ansvaret. Bestemmelsens første ledd fastslår at redaktøren kan holdes ansvarlig for offentliggjøring av innhold som ville ha pådratt ansvar etter et annet straffebud om han hadde kjent til innholdet. Dette er altså et strafferettslig kontrollansvar:

> *«Den som treffer avgjørelse om innholdet i et trykt skrift eller en kringkastingssending, er strafferettslig ansvarlig dersom det der offentliggjøres noe som ville ha pådratt redaktøren ansvar etter noen annen lovbestemmelse om han hadde kjent til innholdet.»*

Tidligere har det eksistert en kobling mellom skadeerstatningsloven § 3-6 som oppstilte en hjemmel for erstatnings- og oppreisningsansvar for redaktøren, og bestemmelsene om straffbare handlinger. Skadeerstatningsloven § 3-6 slo fast at den som hadde krenket en annens ære skulle betaling erstatning «så fremt han har utvist uaktsomhet eller vilkårene for straff ellers er tilstede». Denne henvisningen til straff pekte den gang til straffeloven § 431, som i dag er avløst av § 269. Avkriminaliseringen omtalt ovenfor innebærer at det ikke lenger eksisterer noe straffeansvar å hekte det sivilrettslige erstatningsansvaret på. Reglene om ærekrenkelser i den nye bestem-

melsen i skadeserstatningslovens § 3-6 bokstav a oppstiller heller ikke et objektivt kontrollansvaret for den som tar beslutninger om innholdet i en publikasjon, det vi har kjent som redaktøransvaret. Koblingen mot straffeloven er fjernet, ettersom bestemmelsene om straff for ærekrenkelser er luket bort.

Redaktøren vil fortsatt kunne holdes ansvarlig på alminnelig subjektivt grunnlag, der hun har hatt slik befatning med innholdet at ansvarsforholdet fremstår som tilstrekkelig klart. Men dette er altså ikke det samme som et objektiv ansvar slik vi fant i den tidligere henvisningen fra skadeserstatningsloven til straffebestemmelsene i den gamle straffeloven.

Som nevnt ovenfor utviklet det seg en ulovfestet rettstilstand knyttet til reglene om ærekrenkelser, som omfattet både hvordan ytringer og utsagn skulle tolkes, samt innholdet i den etterfølgende rettsstridsvurderingen som måtte innfortolkes i straffebudene. Fra den erstatningsrettslige siden, forelå det imidlertid en klar lovhjemmel når det underliggende strafferettslige ansvarsgrunnlaget var avklart. Når selve erstatningshjemmelen ble fjernet, er det vanskelig å se at det er rom for noen ulovfestet lære knyttet til selve redaktøransvaret som sådan. Her forelå det altså en lovfestet ansvarshjemmel, og når denne først er blitt fjernet av lovgiver kan den ikke gjenoppstå ved en enkel henvisning til den tidligere ulovfestede rett som har supplert lovreguleringen.

Konklusjonen må dermed være at vi per i dag ikke har et slikt erstatningsansvar i Norge, der redaktøren står erstatningsansvarlig under et objektivt kontrollansvar. Dette synspunkt er også blitt lagt til grunn i Oslo tingretts dom av 30. juni 2017, i den såkalte Hjernekirurg-saken som gjaldt nettopp krav om erstatning etter påstått ærekrenkelse.

> *« Ved endringen av straffeloven og skadeerstatningsloven forsvant koblingen mellom skadeserstatningsloven og straffeloven. Etter at koblingen forsvant gjelder redaktørens kontrollansvar (objektive ansvar) kun straffeansvaret og ikke erstatningsansvaret.»*

For redaktørene er dette ved første øyekast en lykkelig situasjon, ansvaret er i dag redusert i forhold til tidligere. Virkeligheten er imidlertid ikke så enkel. Redaktørens rolle som endelig beslutningstager er viktig i forhold til publikasjonens selvstendighet og funksjon som uavhengig informasjonsformidler, samt at den legitimerer innholdet som formidles ved at det til enhver tid foreligger en som står ansvarlig. Da vil det kunne være ønskelig med en regulering som omfatter ikke bare det strafferettslige, men også det økonomiske ansvar.

Det jobbes for tiden med en ny medieansvarslov, som forventes å rydde opp i denne situasjonen. Her vil også andre sider ved redaktørens ansvar kunne avklares, for eksempel spørsmål knyttet til ansvarsforholdene der det publiseres krenkende debattutsagn på publikasjonens nettsider. Det eksisterer i dag en spenning mellom e-handelslovens regler om ansvarsfrihet for tjenesteytere på den ene side og på den annen side praksis fra EMD i slike saker. EMD har åpnet for et objektivt ansvar rettet mot selve publikasjonen i flere konkrete avgjørelser, og spørsmålet er nå hvordan dette skal håndteres i den nasjonale lovgivningen. Skal publikasjon eller redaktør holdes ansvarlig, og hvordan kan en slik regulering utføres i tråd med e-handelsdirektivets forutsetninger om at det ikke skal innføres kontrollsystemer som innskrenker tjenesteyterens ansvarsfrihet.

Fredrik Bergsmark Grimstad

The Right to Data Portability in Article 20 of the General Data Protection Regulation: An analysis of the legal obligations for data controllers when data subjects requests the right to data portability

Masteroppgave,
Universitetet i Oslo.
1.12.2017

Fredrik Bergsmark Grimstad.

Masteroppgaven består av en analyse av hvilke juridiske forpliktelser behandlingsansvarlig har dersom en enkeltperson (den registrerte) påberoper seg retten til dataportabilitet etter EUs personvernforordning (GDPR) artikkel 20.

Europakommisjonen har uttalt at med økende bruk av visse online tjenester blir mengden av personopplysninger som samles inn i tjenesten, et hinder for å bytte til en annen tilsvarende tjeneste. I henhold til forordningens fortale punkt 68, har dataportabilitet til formål å styrke enkeltpersoners kontroll over egne personopplysninger. Masteroppgaven inneholder en forklaring av hovedelementene til dataportabilitet, udefinerte begreper og generelle rettigheter etter forordningen, som for eksempel krav til informasjon, identifisering og sikkerhet.

Videre omhandler analysen særlig når retten til dataportabilitet gjelder, herunder de kumulative vilkårene om 1) behandlingsgrunnlag (samtykke eller kontrakt), 2) personopplysninger om, og gitt av den registrerte og 3) rettigheter og friheter for tredjeparter. Analysen tar særlig opp hvilke personopplysninger som behandlingsansvarlig er pliktig til å inkludere i utøvelsen av dataportabilitet. Dette gjelder særlig hva som bør forstås som «gitt av» den registrerte, herunder opplysninger som er direkte gitt av enkeltpersonen, men også opplysninger som gis indirekte ved bruk av tjenester. Aktiviteter som blir logget av helseklokker (tingenes internett) blir brukt som et eksempel for en grensedragning av hva som bør forstås som «gitt av» enkeltpersonen.

Funnene i masteroppgaven gir en indikasjon av pliktene for behandlingsansvarlige etter retten til dataportabilitet. Behandlingsansvarlig bør allerede nå forberede seg på hvordan vedkommende håndterer en påberopelse av dataportabilitet. Hovedregelen er at behandlingsansvarlig skal besvare henvendelser om dataportabilitet senest én måned fra mottakelse. Brudd på dataportabilitet kan medføre den strengeste sanksjonen i medhold av forordningen.


Wiersholm
Rune Opdahl
Henrik Aakrann

100 dager til GDPR trer i kraft - Ny statusrapport fra Kommisjonen

Den 24. januar kom EU-kommisjonen med en meddelelse til Parlamentet og Rådet om den kommende personvernforordningen («GDPR»), rett over 100 dager før GDPR trer i kraft. Meddelelsen inneholder dels en statusrapport over arbeidet så langt, dels en redegjørelse for veien videre.

Kommisjonen fremhever særlig arbeidet for en styrking av personvernet utenfor EU. De jobber for tiden med en modernisering av Europarådets Konvensjon 108, som er den eneste bindende multilaterale avtalen om personvern. Intensjonen med moderniseringen er at konvensjonen skal bygge på samme prinsipper som GDPR.

Det internasjonale arbeidet er viktig for å bygge bildet av EU som den fremste aktøren på personvern, men er også av stor kommersiell betydning. Det overføres store mengder personopplysninger ut av EU i dag. Å gjøre slike overføringer enklest mulig vil medføre kostnadsreduksjoner. Kommisjonen arbeider derfor også for tiden med prosesser for å godkjenne overføring av personopplysninger til viktige handelspartnere, særlig i Asia og Latin-Amerika, uten at det kreves særskilte tiltak for å beskytte personopplysningene (såkalte «adequacy decision»).

I Kommisjonens meddelelse fremheves det videre at medlemsstatene har et særlig ansvar for å sørge for effektiv implementering av GDPR. Kommisjonen er tydelig på at dersom medlemsstatene ikke følger opp implementeringen, så vil det få konsekvenser. I ytterste konsekvens vil det reises sak for EU-domstolen. Særlig fremheves medlemsstatenes ansvar for å sørge for:

1. At nasjonale regler som implementeres er i samsvar med GPDR og ikke innebærer noen hindringer for anvendelsen av regler i GDPR.
2. At de nasjonale datatilsynene gis tilstrekkelige økonomiske og menneskelige ressurser.
3. Informasjonsarbeid for å øke bevisstheten om det kommende regelverket, særlig blant små og mellomstore bedrifter.

Som del av informasjonsarbeidet har Kommisjonen selv utarbeidet en nettressurs som er spesielt rettet mot små og mellomstore selskaper. Mye av informasjonen om GDPR er lite tilgjengelig, og det er derfor et viktig initiativ. Det er imidlertid foreløpig sparsomt med innhold på siden. Vi får derfor håpe Kommisjonen følger opp og oppdaterer den med mer innhold fremover, slik de antyder at de vil gjøre.

Rune Opdahl er partner og advokat i Wiersholm, Oslo.
Henrik Aakrann er advokatfullmektig i Wiersholm, Oslo.

Gorrissen Federspiel

Tue Goldschmieding

1.1 Vedtagelse af den nye databeskyttelseslov i dansk ret

Det danske justitsministerium ('Justitsministeriet') fremsatte den 25. oktober 2017 et lovforslag vedrørende den nye danske databeskyttelseslov. Anden behandling af lovforslaget forventes igangsat den 8. februar 2018. Den tiltænkte lov skal supplere og gennemføre Europa-Parlamentets og Rådets forordning nr. 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ('Databeskyttelsesforordningen').

Efter den 25. maj 2018 vil det i Danmark være reglerne i Databeskyttelsesforordningen, suppleret af den påtænkte danske databeskyttelseslov, som regulerer området for behandling af personoplysninger. I vidt omfang viderefører lovforslaget de gældende regler, som findes i den danske lov nr. 429 af 31. maj 2000 (' Persondataloven').

Læs hele lovforslaget her:
http://www.ft.dk/ripdf/samling/20171/lovforslag/l68/20171_l68_som_fremsat.pdf

1.2 Artikel 29-gruppen sender vejledning om samtykke i offentlig høring

Den 28. november 2017 sendte Artikel 29-gruppen en vejledning om samtykke i offentlig høring. Vejledningen indeholder en dybdegående gennemgang af betingelserne for et gyldigt samtykke og de begreber, der knytter sig hertil.

Efter Europa-Parlamentets og Rådets forordning nr. 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ('Databeskyttelsesforordningen'), er et gyldigt samtykke betinget af, at det er: 1) frivilligt, 2) specifikt, 3) informeret, og 4) givet ved en utvetydig viljestilkendegivelse.

Som en generel regel, udtaler Artikel 29-gruppen, at et samtykke ikke er gyldigt, når den registrerede ikke har andre valg, føler sig tvunget eller vil blive udsat for negative konsekvenser, hvis de ikke samtykker. Artikel 29-gruppen beskriver bl.a. hvilke informationer, som den registrerede som minimum skal informeres om før samtykket anses for at være informeret. I denne forbindelse bør den dataansvarlige sikre sig, at disse informationer kommunikeres ud på et tydeligt og letforståeligt sprog.

Et gyldigt samtykke udgør en blandt flere forskellige behandlingshjemler. Artikel 29-gruppen udtaler i den forbindelse, at det altid bør overvejes, hvorvidt samtykke er det mest egnede grundlag for den påtænkte behandling af persondata. Samtykke kan være uhensigtsmæssigt i situationer, hvor der er en ubalance i magtforholdet mellem den dataansvarlige og den registrerede. Vejledningen nævner offentlige myndigheder og ansættelsesforhold som eksempler. I det førstnævnte tilfælde vil den registrerede oftest ikke have andre realistiske alternativer end at samtykke til databehandlingen, og i det sidstnævnte tilfælde, vil den ansatte ofte samtykke ud fra frygten for skadelige konsekvenser.

Læs udkast til vejledning her:
https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/wp259_samtykke_en.pdf

1.3 Artikel 29-Gruppen sender vejledning om gennemsigtighed i Persondataforordningen i høring

Artikel 29-gruppen har sendt en vejledning om gennemsigtighed i databehandling og oplysningsforpligtelser i Europa-Parlamentets og Rådets forordning nr. 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF ('Databeskyttelsesforordningen') i høring. Vejledningen vedrører hovedsageligt Databeskyttelsesforordningens artikel 13 og 14 om oplysningsforpligtelser ved indsamling af persondata hos den registrerede og andre.

Gennemsigtighed skal sikre den registreredes mulighed for at holde databehandlere ansvarlige samt give mulighed for at udøve den kontrol, man som registreret har ret til at udøve. Vejledningen vil fungere som ledesnor for praktikere samt bidrage til fortolkning af de pågældende bestemmelser.

Udover retningslinjer til forståelsen af artikel 13 og 14 giver vejledningen også oplysninger om artikel 12's indhold. Det uddybes, hvad der

menes med "kortfattet, gennemsigtig, letforståelig og lettilgængelig", "klart og enkelt sprog", "gratis" mv. Derudover indeholder vejledningen både eksempler på 'good practice' og 'bad practice'.

Høringsfrist angående vejledningen er den 23. januar 2018.

Læs udkast til vejledning her:
https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/wp260_gennemsigtighed_en.pdf

1.4 Artikel 29-gruppen sender arbejdsdokumenter om mulighederne for overførsel af data til tredjelande i offentlig høring

Artikel 29-gruppen har sendt tre arbejdsdokumenter til høring med høringsfrist den 17. januar 2017. Arbejdsdokumenterne omhandler mulighederne for overførsel af persondata til tredjelande. Dokumenterne indeholder opdateringer af eksisterende arbejdsdokumenter som følge af implementeringen af Europa-Parlamentets og Rådets forordning nr. 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ('Databeskyttelsesforordningen').

Det første arbejdsdokument (WP254) omhandler tilstrækkeligt databeskyttelsesniveau i et tredjeland og opdaterer det gældende arbejdsdokument (WP12). Artikel 29-gruppen opstiller i dette arbejdsdokument en række databeskyttelsesprincipper, der som minimum bør gælde i et tredjeland og hos internationale organisationer for at være i overensstemmelse med EU-retlige regler om overførsel af persondata til et tilstrækkeligt sikret tredjeland.

De øvrige to arbejdsdokumenter (WP 256 og 257) vedrører elementer og principper, som skal være indeholdt i et sæt bindende virksomhedsregler for henholdsvis databehandlere og dataansvarlige. Artikel 29-gruppen revurderer de tidligere gældende arbejdsdokumenter i overensstemmelse med Databeskyttelsesforordningen og opstiller principper og elementer, der bør være indeholdt i de dokumenter, som udgør virksomhedens bindende virksomhedsregler (også kaldet BCR).

Læs udkast til arbejdsdokumenterne her:
https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/wp254_tilstraekkelighed_en.pdf
https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/wp256_bcr_en.pdf
https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/wp257_bcr_p_en.pdf

1.5 Kommissionens evaluering af Privacy Shield-aftalen

Den 18. oktober 2017 udgav EU-Kommissionen sin første årlige evaluering af Privacy Shield-aftalen. Rapporten er udarbejdet af embedsmænd fra EU og USA. Rapporten konkluderer, at Privacy Shield-aftalen har bidraget til et højnet databeskyttelsesniveau, men indeholder samtidig anbefalinger til forbedringer.

Indledningsvist viser rapporten, at certifikationsproceduren er blevet håndteret på tilfredsstillende vis. Over 2400 selskaber var allerede blevet certificeret, og de amerikanske myndigheder har skabt et system, som kan håndtere klager, håndhæve aftalen og beskytte de registreredes rettigheder.

På følgende områder fandt rapporten dog, at der er plads til forbedringer: i) løbende undersøgelser af falsk anvendelse af certifikater; ii) løbende undersøgelser af om de certificerede lever op til aftalen; og iii) en større indsats for at oplyse registrerede om deres rettigheder.

Rapporten blev efter sin udgivelse sendt til Europa Parlamentet, Rådet, artikel 29-gruppen og relevante amerikanske myndigheder. Kommissionen skal sammen med de amerikanske myndigheder følge op på anbefalingerne.

Læs hele evalueringen her:
http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619

1.6 Den danske rigsrevision kritiserer 3 regioners beskyttelse af adgang til it-systemer og sundhedsdata

Den danske rigsrevision ('Rigsrevisionen') fandt, at der var mangler i regionernes tiltag mod hackerangreb, samt at beskyttelsen af adgangen til it-systemer og sundhedsdata ikke var tilfredsstillende.

I sin beretning, som baseres på IT-revisioner udført i første halvår af 2017, har Rigsrevisionen undersøgt Region Syddanmark, Region Midtjylland og Region Hovedstadens sikringstiltag til beskyttelse mod hackerangreb og begrænsning af medarbejdernes adgang til borgernes sundhedsdata. Særligt kritisk var det, at ledelsen af Region Syddanmark ikke har udarbejdet klare retningslinjer for it-sikkerheden på de områder, som blev undersøgt. Undersøgelsen viser også, at regionerne har fokus på nedbringe mængden af system- og servicekonti, der har privilegerede rettigheder, hvilket vil mindske risikoen for, at hackere kan misbruge medarbejdernes rettigheder.

Læs hele beretningen her:
http://www.ft.dk/~/media/sites/ft/pdf/organisation/folketingets-institutioner/statsrevisorene/2017/beretning-4-2017-om-3-regioners-beskyttelse-af-adgangen-til-it_systemer-og-sundhedsdata.ashx?la=da

1.7 Datatilsynet i Danmark m.fl. udgiver vejledninger om dataansvarlige og databehandlere, samtykke, databeskyttelsesrådgivere og overførsel af personoplysninger til tredjelande

Det danske datatilsyn ('Datatilsynet') udgav i september og november 2017 vejledninger vedrørende en række forhold som private virksomheder og offentlige myndigheder skal overholde ved behandling af personoplysninger, som følge af implementeringen af Europa-Parlamentets og Rådets forordning nr. 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ('Databeskyttelsesforordningen').

I 'Vejledningen om databeskyttelsesrådgivere' redegøres for de krav databeskyttelsesforordningen opstiller til at udpege en databeskyttelsesrådgiver, databeskyttelsesrådgiverens opgaver, kvalifikationer, stilling og inddragelse.

'Vejledningen om dataansvarlige og databehandlere' indeholder generelle principper som private virksomheder, offentlige myndigheder, fysiske personer, institutioner og andre organer kan bruge som hjælp, når de skal vurdere, hvorvidt de behandler persondata som dataansvarlig eller databehandler.

I 'Vejledningen om samtykke' redegøres der for, hvornår der foreligger et gyldigt samtykke, og hvad retsvirkninger er, hvis et samtykke trækkes tilbage af den registrerede. Endvidere redgøres der for de helt nye regler i Databeskyttelsesforordningen, om børns samtykke i forbindelse med informationssamfundstjenester.

'Vejledningen om overførsel af personoplysninger til tredjelande' redegør for de særlige regler i Databeskyttelsesforordningen, der regulerer situationer, hvor virksomheder og myndigheder i forbindelse med deres behandling af personoplysninger, overfører personoplysninger til et tredjeland.

Læs alle vejledningerne her:
https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_om_dataansvarlige_og_databehandlere_-_endelig_version.pdf
https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledning_om_samtykke__formateret_.pdf
https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_DPO.pdf
https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_om_overfoersel_til_tredjelande_-_endelig_version.pdf

1.8 Danske offentlige myndigheder udsteder informationspjece om Databeskyttelsesforordningen

Det danske datatilsyn ('Datatilsynet') og det danske justitsministerium ('Justitsministeriet') samt den danske digitaliseringsstyrelse ('Digitaliseringsstyrelsen') og den danske erhvervsstyrelse ('Erhvervsstyrelsen') offentliggjorde den 10. oktober 2017 en informationspjece om Europa-Parlamentets og Rådets forordning nr. 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ('Databeskyttelsesforordningen'). Pjecen er nummer tre i en serie af vejledninger, som myndighederne har forpligtet sig til at offentliggøre inden slutningen af 2018.

Formålet med vejledningen er at introducere de nye databeskyttelsesregler i hovedtræk. Vejledningen indeholder blandt andet vejledning om, hvornår forordningen gælder, hvilke oplysninger, der betragtes som persondata, hvad der anses som behandling, hvornår behandling må finde sted, samt de registreredes rettigheder og kravene til behandlingssikkerhed.

Vejledningen indeholder også et afsnit om andre særlige nyskabelser under Databeskyttelsesforordningen, blandt andet kravet om at føre fortegnelser over behandling af personoplysninger, og regler om virksomheders udarbejdelse af konsekvensanalyser forud for databehandlinger.

Læs hele pjecen her:
https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Captia_Generel_informationspjece__formateret___DOK446249_.pdf

1.9 Datatilsynet i Danmark udtaler kritik af statslige myndigheders brud på persondataloven

Det danske datatilsyn ('Datatilsynet') har i forbindelse med dets tilsynsvirksomhed afsløret en række statslige myndigheders brud på den danske lov nr. 429 af 31. maj 2000 om behandling af personoplysninger ('Persondatalov'), og udtalt kritik af disse myndigheder.

Stikprøven viste, at 7 ud af 8 myndigheder under tilsyn havde omfattende eller meget omfattende mangler ved deres databeskyttelse. Datatilsynets kontorchef kom derfor med en opfordring til alle danske myndigheder og virksomheder om at sætte mere fokus på databeskyttelse.

Det danske beskæftigelsesministerium ('Beskæftigelsesministeriet') var blandt de statslige myndigheder, hvis databeskyttelse havde meget omfattende mangler. Datatilsynet konkluderede blandt andet, at Beskæftigelsesministeriet ikke konsekvent havde efterlevet kravet om årlig gennemgang af egne uddybende sikkerhedsregler eller fastsat fornødne retningslinjer for eget tilsyn. Endvidere havde ministeriet kun for under halvdelen af de anvendte databehandlere indgået en skriftlig databehandleraftale og påset sikkerheden.

Læs alle afgørelserne her:
https://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/Tilsyn-med-Beskftigelsesministeriet/
https://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/tilsyn-med-vejdirektoratet/
https://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/tilsyn-med-udbetaling-danmark/
https://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/Tilsyn-med-Sundhedsdatastyrelsen/
https://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/tilsyn-med-sundheds-og-aeldreministeriet/
https://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/tilsyn-med-rigspolitiet/
https://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/Tilsyn-med-Udlndinge-og-Integrationsministeriet/
https://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/tilsyn-med-rigsadvokaten/

1.10 ENISA udgiver årlig rapport om tilsyn og sikkerhedsbrud

Det Europæiske Agentur for Net- og Informationssikkerhed ('ENISA') udgav den 29. november 2017 en rapport om det forudgående kalenderårs tilsynsvirksomhed i henhold til artikel 19 i forordning (EU) 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked. Dette er den først rapportering, og derfor dækker rapporten kun sidste halvdel af 2016.

De årlige rapporteringer skal blandt andet indeholde en sammenfatning af de indberetninger om brud på sikkerheden, som tillidstjenesteudbydere har modtaget.

2016 var tilsynsvirksomhedens første rapporteringsår, og i anden halvdel af 2016 blev kun én hændelse indberettet til ENISA. Dette sikkerhedsbrud skyldtes systemfejl, hvilket er blevet identificeret som den mest hyppige årsag til brud på sikkerheden i de forudgående seks år af ENISA i deres årlige rapport for 2016 om sikkerhedsbrud i Europa inden for den elektroniske kommunikationssektor. Da der kun forelå denne ene rapportering, indeholder rapporten en mere dybdegående behandling af selve rapporteringssystemet.

Læs hele rapporten her:
https://www.enisa.europa.eu/publications/annual-incident-analysis-report-for-the-trust-service-providers

1.11 ENISA udgiver rapport med anbefalinger om certificeringsmekanismer og databeskyttelsesmærkning

Det Europæiske Agentur for Net- og Informationssikkerhed ('ENISA') udgav den 27. november 2017 en rapport om certificeringsmekanismer og databeskyttelsesmærkning. Formålet er at identificere og undersøge udfordringer og muligheder for certificering med særlig fokus på mærkning efter Europa-Parlamentets og Rådets forordning nr. 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ('Databeskyttelsesforordningen').

ENISA anbefaler, at EU-Kommissionen og Det Europæiske Databeskyttelsesråd vejleder og støtter de nationale certificeringsorganer og tilsynsmyndigheder i at forfølge et fælles mål om oprettelse af certificeringsmekanismer efter Databeskyttelsesforordningen. EU-Kommissionen og Det Europæiske Databeskyttelsesråd bør endvidere, i tæt samarbejde med nationale certificeringsorganer og tilsynsmyndigheder, fremme erfaringsudveksling om 'best practices' på veletablerede områder for certificering.

ENISA anbefaler også, at Det Europæiske Databeskyttelsesråd, i tæt samarbejde med nationale certificeringsorganer og tilsynsmyndigheder, fremmer en EU-retlig tilgang til certificering baseret på brede kriterier.

Derudover anbefaler ENISA, at EU-Kommissionen og Det Europæiske Databeskyttelsesråd tilskynder beskyttelsesforanstaltninger i forbindelse med certificeringsprocessen.

Læs hele rapporten her:
https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification

1.12 ENISA udgiver rapport med grundlæggende sikkerhedsanbefalinger til "Internet of Things"

I november 2017 udgav det Europæiske Agentur for Net- og Informationssikkerhed ('ENISA') rapport om grundlæggende anbefalinger for sikkerhed indenfor IoT ('the Internet of Things'). Rapportens anbefalinger er henvendt mod virksomheder og er ment som en vejledning.

Ved sin rapport har ENISA søgt at udarbejde grundlæggende 'cyber security' anbefalinger, med fokus på informationsinfrastrukturer. Disse infrastrukturer kan for eksempel omhandle helbreds-, økonomiske- og eller sikkerhedsinformationer.

Overordnet kan blandt rapportens anbefalinger nævnes, at: i) der bør ske harmonisering i regulering af internet sikkerhed; at ii) bevågenheden omkring 'cyber security' bør øges og; at iii) software/hardware under sin udvikling bør sikre vejledningerne efterleves.

Læs hele rapporten her:
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

1.13 EDPS udgiver refleksionsindlæg om interoperabilitet mellem informationssystemer inden for områderne frihed, sikkerhed og retfærdighed

Den Europæiske Tilsynsførende for Databeskyttelse ('EDPS') offentliggjorde den 17. november 2017 et

refleksionsindlæg om interoperabilitet mellem informationssystemer inden for områderne frihed, sikkerhed og retfærdighed. EDPS fremhæver, at EU har mødt modgang i form af terroristangreb og massiv indvandring. Dette har medført fokus på interoperabilitet fra EDPS' side i form af ønsket om at udvikle effektiv vidensdeling i mellem medlemsstaternes myndigheder.

EDPS støtter interoperabilitet, såfremt implementeringen heraf er nøje planlagt og overholder de grundlæggende krav om nødvendighed og proportionalitet. Selvom konceptet har en teknisk karakter, bør det ikke være usammenhængende med kravene til dataudveksling. EDPS lægger i den forbindelse vægt på, at overholdelse af databeskyttelsesreglerne vægter højere end kravet om 'privacy by design and by default'. EU-Kommissionen bør derfor nøje overveje, hvilke problemer interoperabilitet skal løse, og hvilken indflydelse det har på behandlingen af persondata. EPDS anbefaler en mere detaljeret analyse og beskrivelse, der kan starte en debat med fokus på de fundamentale rettigheder.

Læs hele refleksionsindlægget her:
https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_en.pdf

1.14 EDPS udtaler sig om forslag til forordning om EU-LISA

Den Europæiske Tilsynsførende for Databeskyttelse ('EDPS') offentliggjorde den 9. oktober 2017 en udtalelse om Forordning nr. 1077/2011 om Det Europæiske Agentur for den Operationelle Forvaltning af Store IT-systemer inden for Området med Frihed, Sikkerhed og Retfærdighed (EU-LISA Forordningen), som blev oprettet i 2011, og som har opereret i 4 år.

EDPS anbefaler, at EU-LISA Forordningen ledsages af en deltaljeret konsekvensanalyse om retten til privatliv og retten til databeskyttelse, som fremgår af Den Europæiske Unions Charter om grundlæggende rettigheder. EDPS udtrykker bekymring over, at arkitekturen af IT-systemerne kun kan ændres ved en ændring af selve lovgrundlaget efterfulgt af en konsekvensanalyse og en undersøgelse af den praktiske anvendelighed. EDPS er derfor bekymret over risikoen for, at EU-LISA, som institution, udvikler og bliver vært for en fælles centraliseret løsning for store IT-systemer, som i princippet er decentraliseret.

Læs alle anbefalingerne her:
https://edps.europa.eu/sites/edp/files/publication/17-10-10_eu-lisa_opinion_en_0.pdf

1.15 EDPS offentliggør anbefalinger om specifikke aspekter af den foreslåede E-databeskyttelsesforordning

Den Europæiske Tilsynsførende for Databeskyttelse ('EDPS') offentliggjorde den 5. oktober 2017 en udtalelse om forslag til Europa-Parlamentets og Rådets Forordning om respekt for privatliv og beskyttelse af personoplysninger i forbindelse med elektroniske kommunikation og om ophævelse af direktiv 2002/58/EF (forordning om databeskyttelse inden for elektronisk kommunikation) ('E-databeskyttelsesforordningen').

EDPS sætter i udtalelsen særligt fokus på behovet for at sikre retlig klarhed og et højt beskyttelsesniveau af retten til privatliv og databeskyttelse. EDPS fremhæver herunder vigtigheden af, at E-databeskyttelsesforordningen udarbejdes i overensstemmelse med princippet om fortrolig kommunikation, og at beskyttelsen er tilstrækkelig og i overensstemmelse med den forventede teknologiske udvikling. EDPS ledsager disse bemærkninger med specifikke anbefalinger, som kan bidrage til mere klarhed.

EDPS lægger endvidere vægt på, at beskyttelsesniveauet i den foreslåede E-databeskyttelsesforordning bør være højere end det forudsatte niveau i forordning nr. 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF ('Databeskyttelsesforordningen'). EDPS understreger, at for mange gentagelser fra Databeskyttelsesforordningen bør undgås, men at det må sikres, at samtykkebegrebet får samme betydning som i Databeskyttelsesforordningen.

Læs anbefalingerne her:
https://edps.europa.eu/sites/edp/files/publication/17-10-05_edps_recommendations_on_ep_amendments_en.pdf

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

FØYEN TORKILDSEN ADVOKATFIRMA

Henny Hallingskog-Hultin
Knut Olav Fiane

Artikkel 29-gruppen har gitt ut veiledning om samtykke etter GDPR

Den 27. november 2017 utga Artikkel 29-gruppen veiledning om samtykke etter GDPR (General Data Protection Regulation 2016/679, heretter «GDPR» eller «forordningen»). Samtykke er ett av seks mulige lovlige grunnlag for å behandle personopplysninger etter GDPR, og er definert i forordningens artikkel 4(11) som en «frivillig, spesifikk, informert og utvetydig viljesytring» fra den registrerte om at vedkommende samtykker i behandling av sine personopplysninger. I tillegg oppstiller artikkel 7 ytterligere vilkår for at behandlingsansvarlig kan basere sin behandling på samtykke, blant annet at samtykket skal kunne dokumenteres og at det skal være like lett å trekke et samtykke tilbake som å avgi det. Veiledningen supplerer tidligere utgivelser fra Artikkel 29-gruppen om samtykke etter någjeldende direktiv, og disse vil fortsatt være relevante i den grad de er i tråd med GDPR.

Veiledningen fremhever at samtykke er et verktøy som gir den registrerte reell kontroll over hvorvidt personopplysninger om vedkommende behandles eller ikke. Det presiseres samtidig at samtykke bare kan være et gyldig behandlingsgrunnlag under de omstendigheter hvor den registrerte gis kontroll og kan velge fritt mellom å gi sitt samtykke eller ikke. Behandlingsansvarlig må vurdere om situasjonen er slik at behandlingen ikke kan baseres på samtykke, for eksempel fordi en skjev eller ujevn maktbalanse mellom partene gjør at den registrerte ikke vil ha et reelt valg mellom å avgi samtykke eller la være.

Et praktisk viktig spørsmål for mange har vært om man kan basere seg på samtykker innhentet under dagens regelverk når GDPR trer i kraft 25. mai 2018. Av fortalen til GDPR fremkommer at svaret på dette i utgangspunktet er ja, men at det likevel kreves at «*the manner in which the consent has been given is in line with the conditions of this Regulation*» (fortalens punkt 171). Det er lett å tenke at dette sender oss tilbake til start og at behandlingsansvarlig vil måtte innhente nye samtykker for å sikre at disse er i tråd med GDPR.

Veiledningen gir noen eksempler på når behandlingsansvarlig kan baseres seg på samtykker avgitt under dagens regelverk, og når man må innhente nye samtykker eller finne et alternativt behandlingsgrunnlag. Det nevnes blant annet at GDPR krever at samtykker kan dokumenteres, og dersom behandlingsansvarlig kun har *«presumed consents of which no references are kept»* må nytt samtykke innhentes. Videre krever GDPR at samtykket er en *«statement or a clear affirmative action»*, noe som betyr at dersom den registrerte kun har unnlatt å fjerne avkrysningen av en ferdig avkrysset boks, kan ikke denne unnlatelsen utgjøre et samtykke etter GDPR. En avklaring er at veiledningen presiserer at selv om informasjonen den registrerte fikk på tidspunktet for avgivelsen av samtykket ikke er i samsvar med GDPR artikkel 13 og artikkel 14, gjør ikke dette nødvendigvis at samtykket som sådan er ugyldig. Om behandlingen fortsatt kan baseres på det avgitte samtykke beror blant annet på hvilken informasjon som ble gitt når samtykket ble avgitt under dagens regelverk.

Veiledningen sier også noe om at behandlingsansvarlig vil ha mulighet til å vurdere om behandlingen kan baseres på et annet behandlingsgrunnlag, dersom man kommer til at samtykket innhentet under dagens regelverk ikke er i samsvar med GDPR. Dette siste vil nok være en praktisk løsning for mange.

Uten at det er behandlet her, redegjør veiledningen nærmere for hva som ligger i vilkårene om at et samtykke er frivillig, spesifikt, informert og utvetydig.

Les veiledningen her:
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611232

Henny Hallingskog-Hultin er advokatfullmektig i Føyen Torkildsen, Oslo.

Knut Olav Fiane er advokat og partner i Føyen Torkildsen, Oslo.

Delphi

Ängela Eklund

Datainspektionen tar ställning till konsekvensbedömningar

Datainspektionen publicerade i mitten av januari sin tolkning av genomförandet av konsekvensbedömningar enligt den nya Dataskyddsförordningen. Till övervägande del överensstämmer Datainspektionens bedömning med den som artikel 29-gruppen har presenterat i sin vägledning om konsekvensbedömningar från april 2017.

Datainspektionen ger i sin bedömning instruktioner till hur en konsekvensbedömning ska genomföras. Inledningsvis anger Datainspektionen att för att veta om en personuppgiftsansvarig är skyldig att genomföra en konsekvensbedömning måste först en riskanalys göras. En sådan analys ska baseras på en specifik händelse och varför den utgör en potentiell risk, hur sannolikt det är att händelsen inträffar och hur allvarliga konsekvenserna blir om händelsen inträffar. Datainspektionen menar vidare att sådana riskanalyser måste ske löpande och utöver att beakta risken för de registrerades integritet ska även övriga fri- och rättigheter beaktas så som yttrandefrihet, fri rörlighet och förbud mot diskriminering.

Utöver de krav avseende konsekvensbedömningar som direkt framgår av förordningen anger Datainspektionen i sin vägledning ett antal åtgärder som kan beaktas vid en behandling för att minska riskerna. Utöver att överväga om det finns alternativa sätt att behandla uppgifterna så att riskerna inte uppstår kan organisationen genom att införa aktiva åtgärder såsom autentisering, kryptering, rutiner, åtkomstkontroll, pseudonymisering samt utforma IT-systemen så att inte fler personuppgifter än nödvändigt behandlas, för att minimera riskerna vid behandlingen.

Datainspektionen rekommenderar vidare att organisationer bör motivera och dokumentera de val som gjort genom konsekvensbedömningen och som ligger till grund för behandlingen. Även om det inte finns något tydligt krav i förordningen att offentliggöra resultaten av en konsekvensbedömning uppmuntrar Datainspektionen till transparens för att uppfylla förordningens principer om öppenhet och ansvarsskyldighet.

Konsekvensbedömningar är ett bra verktyg för organisationer för att få en översikt över riskerna med behandlingen av personuppgifter. En rekommendation är därför att börja i ett tidigt skede av behandlingen och att kontinuerligt se över nya risker som kan ha uppkommit.

Ängla Eklund är associate i Advokatfirman Delphi, Stockholm.

Gorrissen Federspiel

Tue Goldschmieding

1.1 Afspilning af musik på danse- og motionshold, i folkeoplysende forening, var ikke offentlig fremførelse

Den danske Højesteret ('Højesteret') afsagde den 30. oktober 2017 dom i sagen mellem Koda og FOF København. Sagen omhandlede, hvorvidt Koda skulle modtage vederlag fra FOF København i forbindelse med afspilning af musik på en række forskellige danse- og motionshold. spørgsmålet var, om der var tale om offentlig fremførelse efter § 2, stk. 3, nr. 3 i den danske lov nr. 1144 af 23. oktober 2014 ('Ophavsretsloven').

Højesteret har ved en tidligere dom fastslået, at lokale gymnastikforeningers træningshold ikke har karakter af offentlig fremførelse. Højesteret fandt ikke grundlag for at behandle FOF Københavns afspilning af musik på danse- og motionshold anderledes. FOF København er en folkeoplysende forening og må derfor ikke drives i kommercielt øjemed. Musikanvendelsen på danse- og motionshold er et væsentligt element i forbindelse med foreningens aktiviteter, men musikanvendelsen er ikke det primære. Holdene består af et mindre antal deltagere, der samles i en lukket kreds. Foreningen kræver tilmelding til et bestemt hold for en sæson, og det er derfor ikke muligt at vælge hold fra og til. Højesteret anså derfor ikke musikanvendelsen for offentlig fremførelse efter Ophavsretsloven § 2, stk. 3, nr. 3, og stadfæstede med denne begrundelse den danske Sø- og Handelsrets dom af 29. august 2016 i sag V-7-16.

Læs hele dommen her:
http://domstol.fe1.tangora.com/page31478.aspx?recordid31478=1471

1.2 Udgivelse af en bog baseret på Leadership Pipeline-teorien var ikke en krænkelse af et ophavsretligt beskyttet værk baseret på samme ledelsesteori

Den danske sø- og handelsret ('Sø- og Handelsretten') afsagde den 5. december 2017 dom i sagen Sirrah ApS ('Sirrah') mod Dansk Psykologisk Forlag A/S ('Psykologisk forlag')samt forfatterne til den omstridte bog. Sagen vedrørte, hvorvidt udgivelsen og markedsføringen af bogen "Leadership Pipeline i den offentlige sektor" ('LPO-bogen') udgjorde en krænkelse af rettighederne til bogen "Leadership Pipeline – How to Build the Leadership Powered Company" (LP-bogen). LP-bogen nyder ophavsretlig beskyttelse efter § 2 i den danske lov nr. 1144 af 23. oktober 2014 ('Ophavsretsloven'). Begge bøger var fagbøger om ledelse baseret på samme ledelsesteori.

Sø- og Handelsretten foretog en tekstuel sammenligning af de to bøger og fandt ikke, at LPO-bogen var en slavisk oversat kopi af LP-bogen eller noget i lighed hermed. Retten fremhævede, at det er almindelig praksis at videreudvikle og afprøve eksisterende teori, men at den valgte teori skal være tydeliggjort. I denne sag var det i LPO-bogen med tilstrækkelig tydelighed anført, hvilken teori der afprøves, og det indholdsmæssige sammenfald mellem de to bøger gik ikke ud over, hvad der er rimeligt og tilladeligt. Flere modeller i LPO-bogen blev undersøgt af retten, men hverken bogens opbygning, kapitelstruktur eller anvendelse af modeller og cases var kritisabel. Retten fandt derfor ingen krænkelse af Ophavsretslovens § 2 eller den danske lov nr. 426 af 3. maj 2017 ('Markedsføringsloven').

Læs hele afgørelsen her:
http://domstol.fe1.tangora.com/media/-300011/files/V007900K.pdf?rev1

1.3 Fire afgørelser fra 'European Union Intellectual Property Office' I kølvandet på den nye EU-varemærkeforordning

Den 26. september 2017 offentliggjorde det Europæiske kontor for Harmonisering i det Indre Marked (Varemarked og Design) ('EUIPO') fire afgørelser som led i anden bølge af lovgivningsreformsprocessen af den nye EU-varemærkeforordning, Europa-Parlamentets og Rådets forordning (EU) nr. 2015/2424 om ændring af varemærkeforordningen ('Ændringsforordningen').

Ændringsforordningen trådte i kraft den 23. marts 2016 og indeholder en række bestemmelser, der gjaldt fra og med 1. oktober 2017, da forordningen måtte udbygges med sekundær lovgivning. EUIPO's afgørelser er et led i denne sekundære lovgivning.

Første afgørelse, EX-17-3, omhandler de formelle krav til et prioriteret krav for et EU varemærke mv. Anden afgørelse, EX-17-5, omhandler de formelle krav til et prio-

riteret krav for at registreret et 'Community design'. Den tredje afgørelse, EX-17-6, omhandler de tekniske krav til bilag indsendt om 'data carriers'. Den fjerde afgørelse, EX-17-7, omhandler metoder til betaling af afgifter og gebyrer, og fastsættelse heraf.

Afgørelserne har virkning fra 1. oktober 2017.

Læs alle afgørelser her: *https://euipo.europa.eu/ohimportal/en/news?p_p_id=csnews_WAR_csnewsportlet&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&journalId=3819981&journalRelatedId=manual/*

1.4 EU-kommissionen udtaler sig om Brexit og immaterielle rettigheder

Europa-Kommissionen offentliggjorde den 6. september 2017 et udspil om immaterielle rettigheder i Storbritannien efter Brexit. Udspillet viser EU's standpunkt i relation til forhandlingerne under artikel 50 i Traktaten om den Europæiske Union og indeholder bud på, hvad udtrædelsesaftalen skal indeholder for at sikre immaterielle rettigheder.

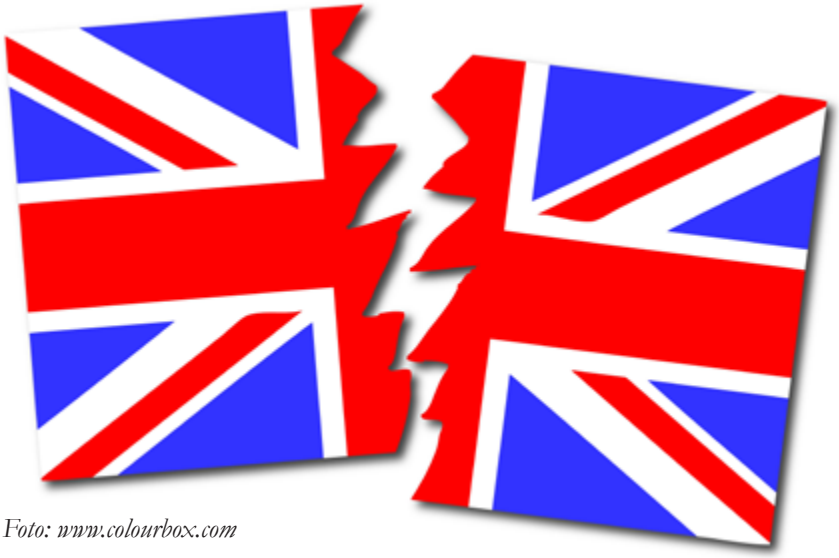

Foto: www.colourbox.com

EU-Kommissionen fremsatte fem bemærkninger til, hvad EU og Storbritannien bør sikre i forbindelse med udtrædelsen. 1) Immaterielle rettigheder beskyttet inden for EU, forud for Brexit, må ikke blive undermineret af Storbritanniens udtrædelse, 2) Procedurerelaterede rettigheder i relation til ansøgninger, herunder prioritetsrettigheder, må ikke gå tabt, 3) Verserende ansøgninger om supplerende beskyttelsescertifikater skal færdiggøres, 4) Beskyttede databaser skal fortsat nyde beskyttelse, og 5) Rettigheder erhvervet før udtrædelsestidspunktet må ikke påvirkes.

Læs hele udspillet her: *https://ec.europa.eu/commission/sites/beta-political/files/position-paper-intellectual-property-rights_en.pdf*

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


simonsen vogtwiig
Hedda Baumann Heier
Rune Ljostad

Oslo tingrett: Utlevering av abonnementsopplysninger til IP-adresser tilknyttet fildelingsnettverk

Den 15. januar 2018 avsa Oslo tingrett kjennelse i sak mellom rettighetshavere og internettilbydere om utlevering av abonnementsopplysninger til IP-adresser tilknyttet fildelingsnettverk. Saken er den første siden forårets høyesterettsavgjørelse i sak HR-2017-833-A (Scanbox), der Høyesterett ikke fant grunnlag for å sette til side lagmannsrettens avgjørelse om å nekte utlevering av abonnementsopplysningene. I den ferske kjennelsen fra Oslo tingrett er resultatet motsatt.

Etter åndsverkloven § 56 b tredje ledd kan domstolene gjøre unntak fra internettleverandørens taushetsplikt etter ekomloven § 2-9 og pålegge utlevering av opplysninger som identifiserer innehaveren av et abonnement. Grunnvilkår for utlevering er at rettighetshaveren fremsetter en begjæring til domstolene og at en krenkelse av opphavsrett eller nærstående rettigheter sannsynliggjøres. Om grunnvilkårene er oppfylt beror utlevering på en interesseavveining der det skal tas hensyn til «krenkelsens grovhet, omfang og skadevirkninger». I Sanbox-avgjørelsen fant Høyesterett at dette tilsa en konkret vurdering i den enkelte sak. Tilgang kan gis hvis overtredelsen er av et «visst omfang», men også andre elementer som grovhet, skadevirkninger og type verk må trekkes inn. Høyesterett fant ikke grunnlag for

Foto: www.colourbox.com

skjematisk anvendelse av bestemmelsen.

I likhet med i Scanbox-saken var det også for Oslo tingrett uomtvistet at opphavsretten til rettighetshaverne var sannsynliggjort krenket ved de aktuelle fildelingene. Det sentrale tvistetemaene var om det var sannsynliggjort deling av et slikt *omfang* at vilkårene for utlevering etter åvl. § 56b tredje ledd er oppfylt. Tingretten tolker Høyesteretts uttalelser i Scanbox-saken som at vilkåret om et «visst omfang» er oppfylt dersom det sannsynliggjøres fildeling ut over deling til etterforskningsprogramvaren. I motsetning til i Scanbox-saken hadde rettighetshaverne for Oslo tingrett ført bevis for slik fildeling ut over delingen til etterforskningsprogramvaren. Dette med ett unntak: For IP-adresser tilhørende virksomheter, institusjoner og myndigheter hadde rettighetshaverne anført at det ikke kunne oppstilles noe krav om deling utover den til etterforskningsprogramvaren fordi personvernhensyn ikke gjorde seg gjeldende med samme styrke. Dette var tingretten ikke enig i, og det var dermed ikke påvist krenkelse av et «visst omfang» for denne gruppen IP-adresser.

Retten fant videre at når det først var påvist krenkelse av et visst omfang, så er utgangspunktet at det bør gis tilgang til opplysninger som identifiserer innehaveren av abonnementet som er brukt ved krenkelsen, med mindre det foreligger konkrete hensyn som trekker den andre veien. Det fant retten ikke grunnlag for i den foreliggende saken.

Innehaverne av abonnementenes eventuelle interesse i å motbevise at de faktisk er de reelle krenkerne, vil bli ivaretatt ved at de i en eventuell senere rettslig prosess vil få anledning til å imøtegå uberettigede an-

klager. Retten fant heller ikke å kunne legge vekt på rettighetshavernes opptreden i etterkant av utleveringen av abonnementsopplysninger i tidligere saker. Ei heller fant retten at et eventuelt fravær av attraktive lovlige tjenester kunne tale mot at opphavsrettskrenkelser kan forfølges etter åndsverkloven § 56b.

Les hele kjennelsen med saksnummer TOSLO-2016-199281 i Lovdatas database. Kjennelsen er i skrivende stund ikke rettskraftig.

Follo tingrett: Økokrim inndrar domenet popcorn-time.no

Økokrim besluttet å inndra domenet «popcorn-time.no» i september 2017. Ettersom registraren av domenet, organisasjonen Imcasreg8, ikke vedtok inndragningsforelegget, ble saken sendt til Follo tingrett. Organisasjonene Norsk Unix User Group og Elektronisk Forpost Norge trådde inn som partshjelpere for registraren.

Tingretten fant det klart at straffeloven gav adgang til inndragningen rettet mot registraren, som besitter bruksretten til domenet, når eieren av domenet er ukjent. Det var heller ikke tvilsomt at et domene kan inndras. Spørsmålene som gjensto for retten å ta stilling til var da:

1) Om popcorn-time.no har vært brukt ved en straffbar handling i form av medvirkning til forsettlig tilgjengeliggjøring for allmennheten av åndsverk uten rettighetshavers samtykke, og under særlig skjerpende forhold.

2) Om inndragning skal foretas, hvor det særlig er lagt vekt på om inndragning er påkrevd av hensyn til en effektiv håndheving av straffebudet og om den er forholdsmessig, jf. straffeloven § 69 tredje ledd.

Retten fant under henvisning til Oslo tingretts kjennelse i sak nr. 17-093347TVI-OTIR/05 og EU-domstolens dom i sak C-527/15 (Filmspeler), at rettighetskrenkelser foretas av eller gjennom Popcorn Time-tjenesten. Retten fant videre at det også forelå særdeles skjerpende omstendigheter på grunn av den store mengden nytt innhold og det særlig brukervennlige brukergrensesnittet. Uten å kvantifisere fant retten det hevet over enhver rimelig tvil at Popcorn Time har påført rettighetshaverne stor skade.

Når det gjaldt spørsmålet om den ukjente eieren av domenet popcorn-time.no har medvirket til den ovennevnte hovedhandlingen, kom retten til at vedkommende hadde gjort det enklere for norske brukere å benytte tjenesten. Domenet var således med på å forsterke virkningen av handlingene til de som sto bak Popcorn Time. De private partene ble ikke hørt med at medvirkningshandlingene lå for fjernt fra hovedhandlingen, og retten var heller ikke enig i at popcorn-time.no kan sammenliknes med en avis eller aktør i en debatt. Innholdet på domenet gikk etter rettens syn langt utover dette.

Retten fant videre at inndragning ville være et egnet og nødvendig middel for å stoppe den straffbare medvirkningen. Inndragning hadde minimale konsekvenser for registraren, mens hensynet til rettighetshaverne tilsa med stor vekt at inndragning må kunne benyttes i et tilfelle som det foreliggende. Hensynet til ytrings- og informasjonsfriheten tilsa ikke en annen løsning. Inndragning er et inngrep som er hjemlet i lov og forfølger legitime formål. Innholdet på popcorn-time.no hadde ikke, etter retten syn, noe særlig vern, og var ikke sammenliknbart med f.eks. hvordan aviser formidler nyheter om Popcorn Time. Noen nedkjølende effekt av inndragningen kunne retten vanskelig se. Retten fant etter dette at vilkårene for inndragning av bruksretten til domenet «popcorn-time.no» var oppfylt.

Les avgjørelsen med saksnummer TFOLL-2017-158053 i lovdatas database. Avgjørelsen er anket.

Rune Ljostad er partner i Advokatfirmaet Simonsen Vogt Wiig AS.

Hedda Baumann Heier er advokatfullmektig i Advokatfirmaet Simonsen Vogt Wiig AS.


Bird & Bird

Jerker Edström
Patricia Otter

Högsta domstolen B 2787-16 Domännamnsförverkandet

I ett nytt avgörande från december 2017 fastställer Högsta domstolen („HD“) att rätten till domännamn utgör egendom som kan förverkas enligt upphovsrättslagen.

Bakgrund

Enligt 7 kap. 53 a § andra stycket lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk („URL“) ska egendom som använts som hjälpmedel vid brott enligt URL få förklaras förverkad, om det behövs för att förebygga brott, eller om det annars finns särskilda skäl. Bestämmelsen tillkom efter beslut av Europeiska unionens råd (Rådets rambeslut 2005/212/RIF av den 24 februari 2005 om förverkande av vinning, hjälpmedel och egendom som härrör från brott) („Rambeslutet“). Enligt förarbetena till bestämmelsen i URL bör det vid frågan „om förverkande behövs för att förebygga brott“ fästas särskilt avseende vid egendomens mer eller mindre utpräglade egenskap av hjälpmedel, omständigheterna vid brottet och egendomens betydelse i sammanhanget. Vidare anges att situationer där det skulle framstå som stötande att gärningsmannen får behålla hjälpmedlet är sådana „särskilda skäl“ som stadgas i bestämmelsen.

Fildelningssajten The Pirate Bay (tillgänglig från domänerna thepiratebay.se, respektive piratebay.se) hade under ett antal år använts för tillgängliggörande av upphovsrättsligt skyddade verk. En grupp personer delaktiga i sajten, däribland klaganden i detta mål („FN“), dömdes år 2010 för medverkan till upphovsrättsintrång genom tillhandahållande av sajten. Enligt åklagaren hade den olagliga verksamheten efter 2010 års dom alltjämt fortsatt. Åklagaren yrkade därför i tingsrätten att rätten till domänerna thepiratebay.se respektive piratebay.se skulle förverkas hos klaganden i dennes egenskap av registrerad och/eller faktiskt innehavare av domänerna. Som grund anförde åklagaren att domänerna sedan 2009 hade använts – och alltjämt användes – som hjälpmedel vid upphovsrättsbrott eller medhjälp till sådant brott. Förverkande, menade åklagaren, kunde därför ske med stöd av 7 kap. 53 a § andra stycket URL eller 36 kap. 3 § p. 1 brottsbalken (1962:700). Tingsrätten fann att förverkande enligt brottsbalken inte kunde ske men bifföll åklagarens yrkande med stöd av förverkandebestämmelserna i URL. Hovrätten fastställde därefter tingsrättens domslut.

Högsta domstolens bedömning

HD konstaterar inledningsvis att egendomsbegreppet är centralt i förverkandelagstiftningen och att

Foto: www.colourbox.com

förmögenhetstillgångar av alla slag, inklusive olika typer av rättigheter, ska förstås som egendom. Domstolen konstaterar vidare att det inte är något krav att egendomen rent faktiskt betingar ett värde, däremot att den ska vara av sådan beskaffenhet att den kan tillhöra någon. Det kan således röra sig om en äganderätt, nyttjanderätt eller annan rättighet. HD konstaterar också att egendom, enligt Rambeslutet, definieras som all slags egendom som styrker äganderätt eller annan rätt till sådan egendom.

Vidare fastslår domstolen att hjälpmedel enligt Rambeslutet ska förstås som all slags egendom som på något sätt, helt eller delvis, använts eller varit avsedd för att begå brottslig gärning eller brottsliga gärningar. Med hänvisning till prop. 2004/05:135 s. 169 menar domstolen att hjälpmedel i URL's mening i princip ska förstås på samma sätt som i 36 kap. 2 § brottsbalken. Det finns således inget krav på att egendomen ska vara av viss karaktär för att den ska kunna utgöra hjälpmedel vid brott. Inte heller krävs det att hjälpmedlet är en förutsättning för att brottet ska komma till stånd eller att det varit särskilt konstruerat eller särskilt lämpat att användas just för brott. I detta sammanhang nämner domstolen också bestämmelsen i 23 kap. 2 § brottsbalken som reglerar när befattning med hjälpmedel kan utgöra förberedelse till brott, eftersom det i förarbetena till denna bestämmelse (prop. 2000/01:85 s. 40 ff. och 49 f.) framhålls att immateriella objekt såsom datavirus och programvara kan utgöra sådana hjälpmedel.

Domstolens första fråga att ta ställning till är om rätten till ett domännamn kan anses utgöra egendom i den mening som avses i 7 kap. 53 a § andra stycket URL. Åklagaren var av uppfattningen att domännamn utgjorde sådan egendom medan klaganden invände att namnet endast utgjorde en adressuppgift.

HD inleder med att konstatera att domännamn huvudsakligen är oreglerade enligt svensk rätt, att ingen enskild stat självständigt har lagstiftat på området samt att de regelverk som finns att tillgå huvudsakligen är privaträttsliga och internationella. HD konstaterar vidare att den som registrerar ett domännamn får en uteslutande rätt att använda detta och att rätten till namnet kan vara föremål för särskild tvistlösning eller talan om bättre rätt. Däremot – konstaterar domstolen – finns det för domänrätten inget sanktionssystem som skyddar ensamrätten motsvarande det som gäller enligt t.ex. varumärkesrätten. Ensamrätten medför inte någon rätt till att använda namnet i något annat sammanhang utöver domänen. Slutligen fastställ-

ler HD i denna del att domännamn är överlåtbara, att det förekommer handel med domännamn samt att de kan ha ett betydande ekonomiskt värde.

HD fortsätter med att titta på Europadomstolens praxis och särskilt målet Paeffgen GmbH v. Germany, dec., nos. 25379/04, 21688/05, 2172205/05 and 21770/05, 18 September 2007 där Europadomstolen fastställde att rätten till ett domännamn är en sådan rätt till egendom som skyddas av artikel 1 i första tilläggsprotokollet av den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Vidare anger HD att Europadomstolen i nämnda fall uttalat att begreppet egendom inte är begränsat till fysiska tillgångar men att det vid tillgångar som inte är fysiska har betydelse om innehavet ger upphov till några ekonomiska rättigheter. Det fann Europadomstolen att ensamrätten till ett domännamn kan göra och ansåg det därför utgöra egendom i bestämmelsens mening.

HD konstaterar fortsättningsvis att beslag av domännamn har förekommit i dansk och norsk rättspraxis samt att domännamn regelbundet beslagtas och förverkas i USA (om dessa leder till en webbplats där piratkopierade produkter säljs). Vidare framhåller HD att den dominerande uppfattningen i den svenska juridiska litteraturen är att domännamn kan utgöra någon form av egendom.

Mot bakgrund av detta konstaterar HD att rätten till ett domännamn är en ensamrätt, att ett domännamn kan vara en tillgång med ett ekonomiskt värde, att det kan överlåtas samt att domännamn fyller en funktion liknande den som ett näringskännetecken har.

Starka skäl talar därför – menar domstolen – för att ett domännamn kan anses vara en rättighet av sådant slag som utgör egendom. Vidare att en sådan bedömning också ligger i linje med internationell rättspraxis. Med bakgrund av detta konstaterar HD således att rätten till ett domännamn är egendom i den mening som avses i 7 kap. 53 a § andra stycket URL.

Domstolen har slutligen att ta ställning till om domännamn kan betraktas som hjälpmedel vid brott mot URL. HD konstaterar att det av Rambeslutet och av förarbetena till bestämmelsen om förverkande i URL framgår att hjälpmedelsbegreppet varken behöver vara begränsat till fysisk egendom eller att hjälpmedlet behöver vara särskilt konstruerat eller lämpat för att användas för brott. Domstolen konstaterar avslutningsvis att det därför inte föreligger något principiellt hinder mot att betrakta ett domännamn som hjälpmedel vid brott mot URL.

HD dock nöjde sig med att konstatera att rätten till ett domännamn utgör egendom som kan förverkas och företog ingen närmare prövning av förutsättningarna i det aktuella fallet. Frågan om de aktuella domännamnen utgjorde hjälpmedel vid upphovsrättsbrott eller medhjälp till sådant brott lämnas således obesvarad med hänvisning till prövningstillståndets utformning.

Kommentarer

I januari 2017 meddelade regeringen att den tillsatt en särskilt utredare som ska överväga om det behövs skärpta straffskalor för de allvarligaste fallen av upphovsrättsintrång och varumärkesintrång („Dir. 2017:4“). I Dir. 2017:4 skriver regeringen att det råder oklarhet om hur immateriell egendom, t.ex. domännamn, ska hanteras efter att det förverkats eftersom att ett förverkande innebär att rätten tillfaller staten. Frågan har därvid uppkommit om staten bör avregistrera domännamnet (och då inte betala för det) samt om det – tvärt emot syftet med förverkande – i så fall riskerar att användas på nytt. Utredaren ska i sin rapport (som redovisas 15 februari 2018, en vecka efter författande av detta referat) analysera konsekvenserna av att immateriell egendom förverkas och överväga om det bör införas bestämmelser för hanteringen av sådan förverkad egendom. I detta ska utredaren beakta de yttrande- och etableringsfrihetsrättsliga konsekvenser sådana förverkanden kan medföra. I ljuset av Högsta domstolens dom B 2787-16 ser vi fram emot utredarens överväganden och slutsatser i dessa frågor.

Jerker Edström är advokat och partner i Bird & Bird, Stockholm.

Patricia Otter är associate i Bird&Bird, Stockholm.

Dan Sørensen

Ny standardavtale for fleksible utviklingstjenester

Den Norske Dataforening (DND) er i ferd med å lansere en ny standardavtale, i tillegg til sin eksisterende PS2000-portefølje, knyttet til programvareutviklingsprosjekter. DND oppgir at PS2000 Smidig og PS2000 SOL kun i begrenset grad egner seg for en smidig gjennomføringsmodell, og at den nye standardavtalen legger til rette for et integrert arbeid mellom partene med større grad av samarbeid, læring og kontinuerlig forbedring, slik at avtalen skal være bedre egnet til prosjekter med en smidig gjennomføringsmodell.

I prosjekter med en smidig gjennomføringsmodell er det ikke uvanlig at leverandørens leveranser er kompetanse og kapasitet basert på vanlige bistandsavtaler eller rammeavtaler, hvor kunden er ansvarlig for prosjektstyringen, prosjektorganiseringen, fremdriften og resultatet – leverandøren har kun en innsatsforpliktelse.

Den nye standardavtalen legger imidlertid opp til en viss fordeling av fremdriftsansvaret og at leverandøren skal ha et medansvar for kontinuerlig forbedring underveis i prosjektet. Selve gjennomføringsprosessen og arbeidsfordeling er derfor i større grad regulert i forhold til vanlige bistandsavtaler, men kunden skal fortsatt ha et resultatansvar.

Standardavtalen beskriver tre hovedprosesser: En løpende «*produktkøprosess*» (kunden beskriver, oppdaterer og prioriterer funksjonalitet/brukerhistorier i produktkøer/oppgavelister), en «*realiseringsprosess*» (design, utvikling, test, kvalitetssjekk og eventuelt produksjonssetting) som gjennomføres i iterasjoner og en «*forvaltningsprosess*» (feilretting, overvåking, brukerstøtte og forvaltning) knyttet til programvare som er satt i produksjon.

Under standardavtalen skal partene avtale en kapasitet i form av antall fulltidsekvivalenter som leverandøren er forpliktet til å levere. Ressursene skal klassifiseres med tanke på erfaring i tillegg til spesifikasjon av kompetanseområder og kompetansekrav. Leverandøren angir hvilke personer som er tilgjengelige innenfor avtalt kapasitet og kompetanse.

Kunden er forpliktet til å benytte avtalt kapasitet, og dette gjøres ved å gjennomføre løpende bestillinger – tilsvarende avrop på en vanlig rammeavtale. Avtalt kapasitet kan justeres opp eller ned innenfor angitte rammer og varslingsfrister. Bestilte ressurser skal inngå i kundens utviklingsteam.

Selv om det legges opp til et tett samarbeid hvor begge parter tilsynelatende skal ha et felles ansvar for fremdrift og styring i prosjektet, bærer likevel avtalen preg av at det uansett er kunden som har det hele og fulle ansvaret. Dette kommer klart frem ved at «*Kunden beslutter sammensetningen av Utviklingsteam og Kunden har ansvaret for å organisere egne ressurser og Leverandørens ressurser i et eller flere Utviklingsteam.*»

Dette organiserings- og fremdriftsansvaret sammenholdt med kundens resultatansvar gjør nok at avtalen likevel ikke skiller seg så mye fra en vanlig bistandsavtale. Fordelen med den nye standardavtalen kan være at partene slipper å utarbeide en regulering av mekanismer for partenes samhandling.

Til tross for at standardavtalen er ment for smidig programvareutvikling, legges det opp til at kunden også kan gjennomføre bestillinger hvor leverandøren likevel skal ha et resultatansvar. Dette skal avtalemessig håndteres ved at avtaleteksten suppleres med en rekke bestemmelser som angitt i den tilhørende veilederen.

Det fremstår som uklart hvordan en slik hybridmodell er mulig å gjennomføre i praksis under standardavtalen. Spesielt gjelder dette hvordan ansvarsforholdene skal håndteres i prosjekter med både utviklingsteam ledet av kunden hvor kunden har et resultatansvar og utviklingsteam ledet av leverandøren hvor leverandøren har et resultatansvar.

Erfaringer viser at slike hybridmodeller skaper en rekke uklare ansvarsforhold og mindre forutsigbarhet enn kunden kanskje hadde håpet på. Det gjenstår imidlertid å se om verktøyene i denne standardavtalen er egnet til å håndtere slike hybridmodeller.

Dan Sørensen er advokatfullmektig i avdelingen for Teknologi & Media i Advokatfirmaet Selmer, Oslo.

KLIMANØYTRAL DISTRIBUSJON B

NORGE P.P. posten

Returadresse:
Lovdata
Postboks 2016 Vika
NO-0125 Oslo
Norge

Nytt fra

LOVDATA

Digital tekstmarkering

Etter innspill fra våre kunder og en lengre periode med utvikling,
er det hyggelig at vi nå kan starte året med lansering
av en svært etterspurt funksjon i Lovdata Pro.

Med tekstmarkeringsfunksjonen i Lovdata Pro
kan du utheve og understreke tekst i flere ulike farger
– og knytte det hele til dine egne merknader.

Nyttig for både advokater, saksbehandlere og studenter.

LOVDATAPRO
Ditt viktigste juridiske arbeidsverktøy