Lov & Data

Nr. 128
Desember 2016
Nr. 4/2016







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*
Web-adresse: *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 HP, Oslo og nestleder i Norsk forening for jus og edb.
Medredaktør er Kari Gyllander, Lovdata.
Redaktører for Danmark er dr.juris Henrik Udsen ved Center for informations- og innovationsret, Københavns universitet og Janne Glæsel, partner i firmaet Gorrissen Federspiel.
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 2016
Norge: nkr 345,- pr. år
Utland: nkr 415,- pr. år
Studenter, Norge: nkr 165,- pr år
Studenter, utland: nkr 220,- pr. år
Alle fritt tilsendt.

Lov&Data sendes gratis til ordinære abonnenter av Lovdata Pro og er medlemsblad for foreningene Norsk forening for jus og edb, Svenska föreningen för IT och Juridik (ADBJ) og Dansk forum for IT-ret. 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 241 013 TRYKKSAK

Persondataforordningen – value for money?

Den 25. maj 2018 får persondataforordningen (forordning (EU) 2016/679) virkning. Selvom der således er halvandet år til, er mange virksomheder og myndigheder allerede nu i gang med at forberede sig på de nye regler. Dette er med god grund. Forordningen indeholder på en række områder skærpede krav til behandlingen af personoplysninger, forventeligt markant højere bøder, krav om udpegning af en DPO (data protection officer) for en række virksomheder og for myndigheder og andre tiltag, der skal skærpe beskyttelsen af personoplysninger. At overholde forordningens nye krav (eller med et godt nordisk ord være »compliant«) vil derfor være både tids- og ressourcekrævende for mange virksomheder og myndigheder.

Der er mange gode grunde til at skærpe beskyttelsen af personoplysninger. Den teknologiske udvikling har muliggjort nye og intensive måder at indsamle, udveksle og bruge personoplysninger på. Snowden-afsløringerne, en række andre sager og bl.a. pressens afdækning af, hvordan oplysninger bruges, har vist, at disse muligheder udnyttes på en mere omfattende måde, end hvad der tidligere har været den gængse opfattelse i offentligheden. Personoplysningers stigende økonomisk betydning giver også stærke incitamenter til en omfattende behandling.

Samtidig med anerkendelsen af behovet for en stærk persondatabeskyttelse, bør vi dog også løbende vurdere, om de ganske betydelige byrder, den europæiske persondataregulering, senest forordningen, pålægger virksomheder og myndigheder, står mål med den opnåede effekt. Dette er en vanskelig vurdering, bl.a. fordi den ideelle beskyttelse af personoplysninger vanskeligt lade sig kvantificere og sammenligne med en opgørelse af økonomiske byrder. Ikke desto mindre er det vigtigt, at sådanne vurderinger løbende foretages. De økonomiske ressourcer er ikke ubegrænsede og beskyttelsesmekanismer, der giver »value for money«, sikrer den stærkeste persondatabeskyttelse, ikke kun på papiret men også i praksis. Regler hvis efterlevelse pålægger virksomheder og myndigheder et stort ressourceforbrug men kun giver en beskeden beskyttelseseffekt underminerer på lang sigt også respekten for persondataretten.

I disse år blæser vindene i retning af en stærk persondatabeskyttelse og den offentlige debat er også præget heraf. Men debatten om, hvorvidt og hvordan vi får mest persondatabeskyttelse for pengene og forordningens effekt i denne henseende, er vigtig. Det er en debat, som fordrer input fra alle aktører, virksomheder, myndigheder, praktiserende persondatajurister, forskere m.fl., og som *Lov&Data* selvfølgelig vil facilitere.

Henrik Udsen

The digital sector and the merger review "enforcement gap" – a net fine-meshed enough to catch Big Data?

av Lars Johansson and Andres Acevedo

Big Data, or in other words, large sets of personal information, is a highly valuable asset. The European Commission has for a long time focused on how companies use, store and trade the personal data itself, but has increasingly started to shift focus to *mergers* between companies owning valuable data. Microsoft's recent acquisition of LinkedIn is one such merger. Should merging companies within the digital sector count on increased scrutiny?

General characteristics of merger review

Basically, all western nations have so called merger control rules. Merger control rules require the parties to a merger to notify the country's competition authority (or similar regulator) about the merger, before implementing the merger. The notification then enables the reviewing authority to, *ex ante*, examine if the merger will have a negative impact on competition (e.g. by enabling the merging parties to use the strengthened market power to raise prices or restrict output). If the reviewing authority considers that the merger will have a negative impact on competition, the authority usually has the right to prohibit the merger or is able to file court action in order to stop the merger.

In additional to national rules on merger control, also the EU commission, acting as a supernational competition agency under EU law, is authorized to review mergers of greater significance and has the power to prohibit the merger if the merger will *significantly impede effective competition*.[1]

Lars Johansson

Andres Acevedo

Each year, tremendous amounts of mergers are implemented within the EU and, naturally, the different competition authorities would never be able to review all mergers. The merger review rules are designed to distinguish between *on the one hand* mergers that from a competition authority's perspective are interesting and trigger a review and *on the other hand* mergers that are uninteresting do not trigger a review. The different merger review rules make this distinction by using various "thresholds".

Different thresholds

The merger review thresholds can be *strict* and they can be *soft*. If a merger does not meet a *strict* threshold, no review is triggered, no matter if the parties or the competition

authorities would have wanted there to be a review. If there is a *soft* threshold, this will allow the parties and/or the competition authority some discretion to decide whether to review the merger. For example, Finland and Denmark have *strict* thresholds only, while Sweden and Norway have *soft* thresholds where the competition authority or the merging parties in some cases can use their discretion to decide if there should be a review.

- *Turnover thresholds* – Probably the most common threshold type is the *turnover* threshold. A merger meets the turnover threshold if the parties to the merger (usually the buying company and the target company) has a turnover (usually each) exceeding the amount of the threshold.
- *Asset thresholds* –Another common threshold is the *asset* threshold (for example used in Russia). A merger meets the asset threshold if the parties to the merger has assets exceeding the value of the threshold.
- *Deal value thresholds* – Another common threshold is the *deal value* threshold (for example used in the US), where the merger meets the threshold if the value of the transaction bringing about the merger exceeds the value of the threshold.
- *Substantive thresholds* – Jurisdictions with *soft* thresholds often combine any of above thresholds with a possibility for the competition authority to review the merger if there are material reasons to do so notwithstanding the threshold not at all or only partly being met.

The EU regulation providing the Commission with the authority to review mergers (the "EUMR"),[2] includes *strict turnover* thresholds. As described above, this means that if the turnover does not meet the threshold, the Commission will not be able to review the merger, even if the Commission consider that the merger can have an impact on competition within the union.

> "The EUMR-thresholds' inability to take into account e.g. Big Data, has by some been called an *enforcement gap*.

The EUMR's turnover thresholds require that the combined worldwide turnover of all the merging firms is over €5 billion (combined), and that the EU-wide turnover for *each* of at least two of the merging firms is over €250 million.[3] The EUMR also has an alternative threshold under which also mergers between companies of a slightly lower combined turnover, $2.5 billion, meets the threshold, if *each* of the merging companies has turnover in several Member States.[4] Furthermore, the EUMR thresholds are not met if all of the merging companies achieve more than ⅔ of the turnover in one and the same Member State.

These current thresholds in the EUMR are fairly high, and catch only mergers where both the buyer and the target company in the merger has significant turnover. Where only one of either the buyer or the target has significant revenues, and the other merging company does not, the merger does not meet the threshold.

Turnover thresholds and the so-called enforcement gap

The rationale behind a turnover-based threshold is that only companies with a significant turnover will be able to excerpt market power in a way that is relevant from a competition perspective; if the parties to a merger have low turnover, these companies will not be able to impede competition in a relevant enough manner for the competition authorities to spend enforcement recourses to investigate the merger. The turnover thresholds in the EUMR restricts the Commission from spending its enforcement resources on mergers where one of the merging companies has insignificant turnover and the merger therefore is unlikely to have any effect for the union citizens.

A strict turnover threshold will not take into account other ways that the merger between two companies can be relevant to the competition on the market, other than its turnover. This means that merger control regimes with strict turnover thresholds will disregard the following aspects:

- *Pipeline products* – Companies with pipeline products (especially relevant in the Pharma sector) may have very low turnover but still be of major significance for future competition, if taking into account its products that will enter the market in the future. Under the EUMR's strict turnover thresholds, a big pharma company may acquire companies with significant pipeline products and expected future revenues to an extraordinary deal value, but still escape merger review scrutiny since the target company does not meet the turnover threshold.
- *Gradual acquisitions* – Larger companies that gradually, in from each other independent transactions acquire smaller companies (e.g. a franchisor gradually acquiring franchisees within a franchise system), will be able to over time acquire companies repre-

senting a considerable market power but escaping merger review scrutiny, since none of the individual acquisitions meet the turnover thresholds. However, the EUMR allows the Commission to during a 2-year period, look at the aggregate turnover, if the gradual acquisitions involve the same buyer and the same seller.

- *Big Data companies* – For many companies within the digital sector, the most important asset the company has is its user data that it collects on users of its services (such as messenger services, payment services, games etc.). This user data may be monetized e.g. by marketing and advertising activities. A company may however build huge amounts of user data before it has started to generate revenues. Acquisitions of companies owning significant user data will therefore not necessarily meet strict turnover thresholds.

The EUMR-thresholds' inability to take into account e.g. Big Data, has by some been called an *enforcement gap*. The enforcement gap has been getting particular attention lately in relation to Big Data acquisitions, where the value in the target not has been its sales and turnover but instead the value of the target's data sets.

One example of what by some is perceived to be a potential enforcement gap in relation to Big Data, is Facebook's acquisition of WhatsApp. Even though the Facebook/WhatsApp-deal was valued at $19 billion and WhatsApp had more than 600 million monthly active users worldwide, it did not meet the EUMR thresholds and was notifiable with the Commission only through a technicality in the EUMR allowing the parties' to voluntarily notify the transaction to the Commission.

Reforming the EUMR thresholds to close the enforcement gap

In order to close what some perceive to be a EUMR enforcement gap, the Commission has recently initiated a consultation to seek feedback on the effectiveness of its current merger control thresholds. There are many conceivable ways in which to close the perceived enforcement gap of the EUMR and it remains to be seen what the result of the consultation will be. One way is to implement *soft* thresholds, similar to the Swedish or Norwegian systems. Another would be to include deal or asset value thresholds where e.g. the value of a target company's datasets can be taken into account.

> Critics may argue that some of the ways to close the enforcement gap will increase uncertainty and cause delay for a large number of transactions within the digital sector.

Critics may argue that some of the ways to close the enforcement gap will increase uncertainty and cause delay for a large number of transactions within the digital sector, without actually entailing any benefits from a competition perspective. They may argue that it is unreasonably difficult to assess the value of e.g. customer data and even more unreasonably difficult to assess how and if such assets have any relevance in reviewing the effects of a merger on competition on the markets.

Striking a good balance in how to design thresholds that takes into account the relevant competitive aspects in the digital markets is undoubtedly a difficult task for the competition regulators going forward. Companies and advisors active in transactions within the digital sectors should be aware that the Commission in the future might get the authority to review e.g. Big Data deals even where the merger does not meet the turnover thresholds. For companies in mergers where the parties are involved in Sweden and Norway, this caution is called for already today. As noted, in these jurisdictions the competition authorities already use *soft* thresholds, and nothing stops the competition authority to initiate a review based on the Big Data assets of the target company provided the buyer is a larger company.

Lars Johansson is a Stockholm-based Partner in Roschier's EU & competition team and the Technology team. He has extensive experience in merger control, cartel investigations and abuse of dominance cases on national and EU level.

Andres Acevedo is a Stockholm-based Associate in Roschier's EU & competition team. His experience includes advising clients in a variety of competition law matters and he regularly works on merger filings in a wide range of industry sectors.

Notes

1 Regulation (EC) No. 139/2004, Article 2.
2 Regulation (EC) No. 139/2004.
3 EUMR Article 1.2.
4 EUMR Article 1.3.

Artikeln är framtagen av flera medlemmar i Cloud Sweden Legal (tidigare Cloud Swedens juridikgrupp). Cloud Sweden Legal utgör ett kompetensnätverk av advokater och andra jurister som tillsammans utreder och diskuterar legala frågor om molntjänster. För mer info om Cloud Sweden Legal vänligen se: cloudswedenlegal.com.

Exit från molntjänster: Juridiska aspekter vid byte av en molntjänst

av Daniel Melin, Hans Nicander, Peter Nordbeck, Anna-Sofia Prevell och Caroline Sundberg


Daniel Melin


Hans Nicander


Peter Nordbeck


Anna-Sofia Prevell


Caroline Sundberg

Inledning

Den allt mer utbredda användningen av molntjänster ger upphov till en rad frågeställningar, såväl juridiska som tekniska och ekonomiska. En viktig, men många gånger förbisedd, frågeställning är vad som händer den dagen då samarbetet mellan kund och molntjänstleverantör avvecklas, s.k. exit. Denna fråga uppmärksammas i en ny rapport från nätverket Cloud Sweden Legal som sammanfattas här.

Skälen till en exit kan vara många och kopplade till omständigheter på molntjänstleverantörens eller kundens sida, men även till omvärldsfaktorer som ingen av parterna råder över.

Oavsett anledningen till en exit har kunden typiskt sett alltid ett övergripande behov av att kunna återfå sin data och ges fortsatt möjlighet att använda denna data med motsvarande funktionalitet. Ur kundens perspektiv är alltså ofta huvudsyftet med en exit-strategi att möjliggöra för kunden att med bibehållen och användbar data övergå till en annan lösning utan att drabbas av orimligt höga kostnader, driftstopp eller olägenheter. Därför bör kunden redan i samband med upphandling av en molntjänst lägga stor vikt vid de frågor som är kopplade till hantering av exit.

Frågor kring exit kan antas få allt större betydelse framöver i takt med den snabbt ökande mängden data som lagras i olika molntjänster. I denna artikel vill vi översiktligt belysa exit och ge exempel på viktiga frågor att hantera vid upphandling och avtalsskrivande. Vårt huvudsakliga fokus i denna artikel är kundperspektivet.

Utlösande faktorer

Kunden bör alltid överväga vilken reglering som är önskvärd för exit utifrån kundens eget behov och jämföra detta med den reglering som molntjänstleverantören erbjuder.

Finns det en möjlighet att komma ur avtalet i förtid i ett läge där kunden enbart p.g.a. egna överväganden, t.ex. på grund av ändrad IT-strategi, önskar lämna den aktuella molntjänsten?

Vilka möjligheter finns att komma ur avtalet på grund av faktorer kopplade till molntjänsteleverantören och den specifika molntjänsten? Exempel på sådana faktorer kan vara en tilltagande frekvens av bristande uppfyllelse av SLA, ändrad ägarbild hos molntjänstleverantören, pris- eller villkorsändringar, förändring av tjänsterna, dataintrång eller andra indikationer på bristande datasäkerhet.

En exit kan även utlösas av omvärldsfaktorer som ingen av parterna råder över, t.ex. förändrad lagstiftning i berörda jurisdiktioner som begränsar kundens möjlighet att använda molntjänster eller force majeure-händelser. Villkoren i avtalet bör även ta hand om dessa situationer.

Personuppgiftsfrågor

Kundens data innehåller ofta personuppgifter och det är inte bara viktigt att reglera hur dessa hanteras under avtalstiden, utan även vad som händer vid en exit. Hanteringen av personuppgifter regleras framförallt av personuppgiftslagen, vilken baseras på det så kallade dataskyddsdirektivet. Från och med den 25 maj 2018 gäller istället dataskyddsförordningen, vilken ersätter nuvarande reglering. Denna framställning utgår dock uteslutande från nu gällande regelverk.

Typiskt sett är det kunden som är personuppgiftsansvarig och har ansvar för att lagstiftningen följs vid hantering av kundens data i molntjänsten. Hanteringen av personuppgifter ska regleras i ett personuppgiftsbiträdesavtal mellan kunden och molntjänstleverantören. Om personuppgiftsbiträdesavtalet baseras på molntjänstleverantörens standardmall är det extra viktigt att kunden ser över och säkerställer att avtalet är lämpligt för det specifika fallet.

Om molntjänstleverantören anlitar underleverantörer som behandlar kundens personuppgifter måste även dessa omfattas av bestämmel-

serna i personuppgiftsbiträdesavtalet, inklusive bestämmelserna om exit. En vanlig reglering är att kunden ger molntjänstleverantören mandat att ingå avtal med underleverantörerna för kundens räkning.

Generellt bör samma principer för personuppgiftsbehandling gälla under perioden då exit genomförs, som under pågående avtalsförhållande. Ett grundläggande krav i personuppgiftslagen är att personuppgifter inte får bevaras längre än nödvändigt. Personuppgiftsbiträdesavtalet behöver därför säkerställa att molnleverantören, inklusive eventuella underleverantörer, inte har åtkomst till personuppgifterna efter avtalets upphörande.

Bestämmelser om exit i molntjänstavtal

Nedan beskrivs översiktligt några av de frågeställningar som aktualiseras i samband med en exit och som därför bör regleras i avtalet.

- **Format (portabilitet):** Det är ofta kritiskt och av stor vikt att återfå data i ett för kunden användbart format så att denna data är läsbar och möjlig att använda i andra sammanhang. Kunden bör också överväga i vilken mån behov finns att ha rätt att begära ut annan information som kan behövas för att kunna använda återlämnad data, såsom loggdata, revisionsdata, accessdata, användardatabas och av kunden genererad metadata. Kunden bör antingen ges rätt att bestämma i vilket format data ska återlämnas, alternativt kan parterna tillsammans specificera ett godtagbart format.
- **Tidpunkt:** Kunden bör kunna kräva ett återlämnande av data i princip när som helst under avtalstiden (möjligen med viss kortare fördröjning).
- **Kostnad:** Eventuell kostnad för att återfå data inom en viss tid och i ett visst format bör regleras i avtalet (gärna i kombination med ett tids- och kostnadseffektivitetsåtagande från leverantören).
- **Mottagare:** Kunden bör ges rätt att anvisa att data ska återlämnas, helt eller delvis, till en tredje part (t.ex. en ny leverantör).
- **Fristående rätt:** Kundens rätt att återfå data i rätt tid, format, etc. bör vara oberoende av andra omständigheter. Molntjänstleverantören bör t.ex. inte ha rätt att hålla inne och neka återlämning av data med hänvisning till utestående icke uppfyllda kontraktsförpliktelser.

> Därför bör kunden redan i samband med upphandling av en molntjänst lägga stor vikt vid de frågor som är kopplade till hantering av exit.

- **Säkerhetskopiering/redundans:** Leverantörens hantering av säkerhetskopiering och säkerhetskopior bör regleras, såsom var data ska lagras och/eller säkerhetskopieras, hur detta ska gå till (konfigurering) och hur och inom vilken tidpunkt kopior ska återfås. Detsamma gäller i vilken utsträckning som leverantören säkerställer sin informationshantering genom redundanta system. Det bör regleras i vilken utsträckning och till vilka priser som återläsningstester ska kunna äga rum. Klargör vidare att leverantören i samband med exit ska bevara säkerhetskopior till dess att kunden erhållit all data, alternativt gett sitt godkännande till att säkerhetskopian raderas (se dock punkten om radering av data och om ansvar nedan).
- **Radering av data:** Leverantören (och eventuella underleverantörer) bör åta sig att i samband med molntjänstens upphörande slutgiltigt radera kundens data (se dock punkten om säkerhetskopia/redundans). För personuppgifter är detta ett obligatoriskt krav.
- **Underleverantörer:** Om molntjänstleverantören anlitar underleverantörer, bör det tydligt regleras att även dessa omfattas av bestämmelserna om exit. Detta gäller inte minst om personuppgifter behandlas i molntjänsten.
- **Support från molntjänstleverantören:** Det bör finnas ett tydligt åtagande att molntjänstleverantören vid exit ska ställa resurser till förfogande, främst för att återföra data, men även för att bistå med assistans kring eventuell migrationsproblematik i samband med exit.
- **Påtryckningsmedel:** Det bör säkerställas att det finns påtryckningsmedel (innehållande av betalning eller motsvarande) om molntjänstleverantören inte uppfyller sina åtaganden vid exit.
- **Lagstiftning:** Molntjänstavtalet bör ta höjd för förändrad lagstiftning inom t.ex. personuppgiftsområdet och för särskilt reglerad verksamhet, d.v.s. om ny reglering ställer nya krav på avtalsparterna, bör avtalet tillåta att bestämmelserna om exit justeras i enlighet med den nya regleringen.
- **Ansvar:** Utöver en väl avvägd generell ansvarsreglering, bör, utifrån ett kundperspektiv, ansvaret för förlust av data ges särskild uppmärksamhet och särregleras i de fall det föreligger ett åtagande av leverantören att säkerhetskopiera eller lagra data och/eller upprätthålla redundanta system.
- **Uppsägningstid:** Avtalet bör inte ge leverantören rätt att avbryta eller avsluta molntjänsten i förtid annat än vid mycket allvarliga (och normalt av en domstol eller skiljenämnd bekräftade) avtalsbrott från kundens sida. Under alla förhållanden bör uppsägningstiden vara av sådan längd att kunden alltid har en reell möjlighet att återta sin data och ordna en alternativ lösning.

Daniel Melin är IT-upphandlare på Statens inköpscentral.

Hans Nicander är advokat vid Nicander Advokatbyrå, Stockholm.

Peter Nordbeck är partner i Advokatfirman Delphi, Stockholm.

Anna-Sofia Prevell är Senior Legal Counsel på Klarna.

Caroline Sundberg är advokat i Delphis ITC/IP-grupp.

Alla är medlemmar av nätverket Cloud Sweden Legal.

JUSNYTT

Halvor Manshaus

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

Presumsjon om kunnskap – lenking på Internett

EU-domstolen har i en prejudisiell avgjørelse trukket opp retningslinjer for lenking til opphavsrettslig vernet materiale som er tilgjengeliggjort uten rettighetshavers samtykke. Avgjørelsen i sak C-160/15 GS Media er avsagt 8. september 2016 og har utgangspunkt i en tvist for nederlandsk Høyesterett vedrørende lenking til bilder som er urettmessig lagt ut på Internett.

Etter at avgjørelsen ble kjent er den blitt tatt til inntekt både for en innsnevring av «lenkefriheten», så vel som en utvidelse av retten til å lenke. Dette er tolkningsresultater som står i diametral opposisjon. For å forstå hvordan dette henger sammen er det nødvendig å se nærmere på avgjørelsen og de konkrete vurderinger som var avgjørende for resultatet. I teksten nedenfor diskuterer jeg ut i fra lenking til og fra nettsider, ettersom det var temaet i denne saken. Lenking på Internett kan imidlertid gjøres i en rekke ulike sammenhenger og på ulike plattformer. Lenking på Twitter, Instagram, Facebook osv. vil alle omfattes på samme måte som en nettside. Som jeg påpeker nedenfor, vil det likevel være et praktisk viktig skille mellom lenking med og uten kommersiell hensikt, altså hvorvidt det lenkes med vinning for øye.

Den underliggende tvisten i denne saken gjaldt nakenbilder av den nederlandske kjendisen Britt Dekker, som ble lekket ut i forkant av en reportasje i bladet Playboy. Sanoma, som er den nederlandske utgiveren av Playboy, hadde fått eksklusiv tillatelse fra fotografen Hermès til å publisere bilder til bruk i bladet som skulle gis ut i desember 2011.

GS Media driver nettstedet GeenStijl som er en blanding mellom blogg, sladrespalte og diskusjonsforum. Den som går inn på nettsiden vil se en rosa logo med GS – GeenStijl og undertekst «Tendentieus, ongefundeerd en nodeloos kwetsend» (*Tendensiøs, ufundert og nådeløst krenkende*). Selve navnet på nettstedet GeenStijl betyr *uten stil*. Med en daglig besøksstatistikk på 230.000 brukere, var dette en av de ti mest besøkte nyhetssidene i Nederland. Den 26. oktober 2010 mottok redaktørene hos GeenStijl en anonym melding med lenke til en elektronisk fil lagret hos den australske skylagringstjenesten Filefactory.com. Denne filen inneholdt de aktuelle bildene som Sanoma hadde fått tillatelse til å publisere. Dette var altså forut for

publiseringen som Sanoma hadde avtalt med fotografen.

Sanoma tok samme dag kontakt med GS Media (v/morselskapet) for å forhindre at bildene ble publisert på GeenStijl, men bildene ble likevel omtalt i en artikkel dagen etter, der også ett av bildene var delvis gjengitt. I avslutningen av artikkelen het det (dansk gjengivelse fra C-160/15 GS Media) *«Og nu linket med de billeder, som*

du sad og ventede på.» Ved å klikke på en lenke tilknyttet teksten ble leseren henvist til Filefactory.com, der en ytterligere lenke åpnet for å laste ned 11 filer som hver inneholdt ett enkelt bilde av Dekker.

Sanoma sendte umiddelbart en ny henvendelse til GS Media, nå med krav om at lenken ble fjernet. GeenStijl svarte ikke på brevet og unnlot å gjøre noe med lenken. Sanoma tok da selv direkte kontakt med Filefactory.com og sørget for at selve billedmaterialet ble fjernet fra lagringstjenesten.

Sanoma fulgte deretter opp videre overfor GS Media, med krav om at selve artikkelen ble fjernet, herunder bildet som var delvis gjengitt, samt kommentarer fra lesere som var blitt publisert i tilknytning til artikkelen. Saken tok deretter en vending som ikke er ukjent i denne type tvister: Bildene dukket nå opp et annet sted.

GeenStijl skrev en ny sak der kravene fra Sanoma ble omtalt, og som ble avsluttet med følgende tekst *«Update: [Britt Geertruida Dekker-]nøgenbilleder, endnu ikke set dem? De findes HEEEER»*. Som i den tidligere artikkelen var det også her en lenke til bildene, men denne pekte nå til Imageshack.com i stedet for Filefactory.com. Sanoma sendte krav til Imageshack.com om å fjerne bildene, og dette ble etterfulgt slik at bildene ble fjernet derfra.

Kort tid senere publiserte GeenStijl ytterligere en artikkel under tittelen *«Bye Bye Vinke Vinke Playboy»*, også denne med en lenke som ga tilgang til de aktuelle bildene. På diskusjonsforumet til GeenStijl ble det deretter skrevet innlegg med ytterligere lenker til andre eksterne nettsteder der bildene nå kunne hentes fra.

På denne tiden hadde Sanoma ennå ikke publisert bildene selv. Dette skjedde først ved utgivelsen av bladet Playboy i desember 2011.

Det ble deretter igangsatt rettslige skritt overfor GS Media som gikk helt til Høyesterett i Nederland. På saksøkersiden sto da Sanoma Media Netherlands BV som gir ut bladet Playboy i Nederland, Playboy Enterprises International Inc og den avbildede Britt Dekker.

Tre spørsmål ble forelagt EU-domstolen for prejudisiell avgjørelse. Sentralt sto spørsmålet om det foreligger en *«overføring til almenheden»*, som omtalt i InfoSoc-direktivet (direktiv 2001/29/EF) artikkel 3 første punkt, der det lenkes til et eksternt nettsted som har publisert innhold uten rettighetshaverens tillatelse. EU-domstolen foretok en samlet vurdering av de tre spørsmålene, og vurderte relevans og betydning av faktiske omstendigheter knyttet til tilgjengeliggjøringen, herunder at

- verket ikke er offentliggjort med samtykke fra rettighetshaver
- lenking gjør det enklere å finne frem til åndsverket der dette ellers ikke er lett tilgjengelig
- den som publiserer lenken visste eller burde ha visst at det ikke forelå samtykke
- rettighetshaveren ikke har samtykket til å publisere åndsverket på nettsiden som tilbyr lenken.

EU-domstolen understreker deretter at et viktig formål med direktivet er å gi rettighetshaverne et effektivt vern, men at dette må balanseres mot blant annet ytrings- og formidlingsfriheten (avsnitt 31). Nøkkelen til å forstå avgjørelsen finner vi i avsnitt 33, der det påpekes at *«Domstolen har endvidere præciseret, at begrebet »overføring til almenheden« indebærer en individualiseret vurdering.»*. Det må altså gjøres en konkret vurdering, der de ulike momentene angitt i listen ovenfor vil kunne ha ulik betydning og vekt avhengig av hvordan saken ligger an. Her aner vi at domstolen ikke legger opp til noe krystallklar regel som kan brukes som sjablong i alle etterfølgende saker. Dette fremheves ytterligere i det etterfølgende avsnitt 34:

> *«Ved en sådan vurdering skal der tages hensyn til flere supplerende kriterier, som ikke er selvstændige, men indbyrdes forbundne i forhold til hinanden. Eftersom disse kriterier i forskellige konkrete situationer kan være til stede i stærkt varierende omfang, skal de anvendes såvel individuelt som i forhold til deres samspil med hinanden.»*

Dette samspillet mellom ulike kriterier innebærer at spørsmålet om lenking til åndsverk må avgjøres individuelt ut i fra de faktiske omstendigheter i den enkelte sak. I tillegg må det sees hen til domstolenes tidligere uttalelser som også trekker opp retningslinjer knyttet til vilkårene om at det skal foreligger en tilgjengeliggjøring *og* at denne skal være rettet mot allmennheten (se særlig sak C-466/12 *Svensson*). I dette ligger blant annet at:

- Allmennheten er ment å beskrive et ubestemt antall mottakere som samtidig utgjør et betydelig antall personer. En lenke som kun går ut til en bestemt personkrets som utgjør et ubetydelig antall personer vil altså skille seg fra en åpen lenke som når ut til mange personer.
- Den ytterligere tilgjengeliggjøringen av verket må enten omfatte en ny teknisk fremgangsmåte som skiller seg fra eventuelle tidligere formidlinger av verket, eller så må den omfatte et nytt publikum som ikke var tatt i betraktning ved den opprinnelige formidling. Det følger av domstolens uttalelse på dette punkt at der verket ikke tidligere er offentliggjort vil enhver tilgjengeliggjøring oppfylle begge disse kravene.

- Det er relevant å se hen til om den tilgjengeliggjøring som finner sted er motivert av profitt eller ikke.

Domstolen viser i avsnitt 40 til tidligere praksis (C-466/12 *Svensson*) som slår fast at det å lenke til et nettsted som fritt gjør tilgjengelig de aktuelle åndsverk ikke innebærer noen ny tilgjengeliggjøring. Dette følger forutsetningsvis av det som er sagt ovenfor om at åndsverket da ikke gjøres tilgjengelig for et nytt publikum eller på en annen teknisk plattform enn forutsatt fra rettighetshaver. I det påfølgende avsnitt 41 trekker domstolen deretter opp et skille mellom *Svensson* og den angjeldende saken *GS Media*, ved at det i sistnevnte ikke forelå noe samtykke for den tilgjengeliggjøring som allerede var gjort. Enhver person som får tilgang til verkene via lenken fra GeenStijl er således «ny», ettersom rettighetshaver ikke kan sies å ha samtykket til noen tilgjengeliggjøring overhodet. Manglende samtykke er altså av betydning ikke bare for den opprinnelige tilgjengeliggjøringen på Internett, men også for den som vil lenke til verket fra et annet nettsted. Motsatt vil et samtykke til åpen publisering på Internett samtidig innebære et samtykke også til lenking fra eksterne nettsteder. Dette klargjøres ytterligere i avsnitt 42:

> *«Når og i den udstrækning dette værk er frit tilgængeligt på en internetside, som hyperlinket giver adgang til, må det lægges til grund, at når indehaverne af ophavsretten til dette værk har givet tilladelse til overføringen, må de have haft for øje, at almenheden udgøres af samtlige internetbrugere.»*

I den videre drøftelse problematiserer domstolen den individualiserte fremgangsmåte beskrevet ovenfor når det gjelder kravet til rettmessig tilgjengeliggjøring. Den som ønsker å publisere en lenke vil kunne møte utfordringer når han skal bringe på det rene om det foreligger samtykke til tilgjengeliggjøring av verket. Det er også på dette punkt at avgjørelsen kan være gjenstand for kritikk, ved at den ikke trekker opp klare regler eller anvisninger men heller henviser til en helhetsvurdering med de momenter som er angitt ovenfor.

> Den som ønsker å publisere en lenke vil kunne møte utfordringer når han skal bringe på det rene om det foreligger samtykke til tilgjengeliggjøring av verket.

Hadde saken ligget annerledes an, ville det neppe vært nødvendig å gå inn på disse vurderingene. *Svensson* ble løst på nettopp rettighetshaverens samtykke til den opprinnelige tilgjengeliggjøring på Internett, som måtte forstås som et samtykke også til lenking. I vår sak var det derimot så åpenbart at det forelå ond tro hos GeenStijl i den forstand at man hadde positiv kunnskap om at de ulike rettighetshavere ikke hadde gitt noe samtykke. Domstolen legger da avgjørende vekt på at direktivets artikkel 3 første ledd forutsetter et sterkt vern. Dette fremgår blant annet av direktivets fortale punkt 9, som er omtalt innledningsvis i avgjørelsen.

Sentralt i dommen står derfor avsnittene 49 til 51 som omtaler situasjoner der kravet til aktsomhet løftes opp slik at man ikke lenger kan forutsette fri lenking til verk som er gjort tilgjengelig på eksterne nettsider.

Der det er klart eller burde være klart at lenken peker til en rettstridig tilgjengeliggjøring av verket, vil lenken utgjøre en selvstendig tilgjengeliggjøring som vil kunne utgjøre et urettmessig inngrep. Det samme gjelder en lenke som har til hensikt å omgå sperrer eller hindre som skal begrense allmennhetens tilgang til verket, for eksempel en såkalt «paywall» på en nettavis som skal sikre at leserne betaler for tilgang til innholdet. I denne saken var det særlig det første alternativet som var aktuelt. Dette er også bakgrunnen for at jeg i denne artikkelen fant det nødvendig å gå gjennom hendelsesforløpet mellom partene, som viser hvilken kunnskap som har ligget hos nettstedet som tilbyr lenken, og hvordan sakens utvikling førte til nye lenker og ytterligere forsøk på tilgjengeliggjøring av verkene.

I tillegg understreker domstolen at et eventuelt profittmotiv for lenkingen også vil kunne løfte aktsomhetskravet. Dette er et element som vil ha stor praktisk betydning, ikke bare for aktører som nettaviser og lignende, men også for en rekke mindre profesjonelle nettsteder som oppebærer inntekter i form av reklame, annonser, abonnementsinntekter og lignende. Her vil jeg som et utgangspunkt anta at dess større inntekt eller grad av profesjonalitet, dess strengere vil aktsomhetskravet være. Det er også av betydning å se hen til den formulering som er brukt i avsnitt 51 på dette punkt:

> *«Når der placeres hyperlinks med vinding for øje, må det forventes af den person, der foretager placeringen, at den pågældende foretager den nødvendige kontrol med henblik på at sikre sig, at det omhandlede værk ikke ulovligt er offentliggjort på det netsted, som disse hyperlinks henviser til, således at det må formodes, at placeringen er foretaget med fuldt kendskab til, at der er tale om et beskyttet værk, og at indehaveren*

af ophavsretten eventuelt ikke har givet tilladelse til offentliggørelsen på internettet. Under disse omstændigheder, og forudsat at denne afkræftelige formodning ikke afkræftes, udgør den handling, der består i at placere et hyperlink til et værk, der ulovligt er offentliggjort på internettet, en »overføring til almenheden« som omhandlet i artikel 3, stk. 1, i direktiv 2001/29.»

Her trekkes det altså opp et viktig skille. Utgangspunktet for en alminnelig nettbruker er at det ikke kan forventes at man tar stilling til om et verk er lagt ut med eller uten rettighetshaverens samtykke. Det ville gå for langt i forhold til ytrings- og informasjonsfriheten å forutsette slike undersøkelser fra alminnelige brukere av Internett, ref. avsnitt 46 i avgjørelsen.

> Det er ikke til å unngå at denne avgjørelsen vil gi grunnlag for diskusjon knyttet til sensur av lenker ved at rettighetshavere potensielt kan få et for effektivt vern.

Dette utgangspunktet blir imidlertid snudd helt rundt for den som tilbyr lenker med et profittmotiv. Sammenhengen her trenger ikke være at man tjener penger på akkurat den ene lenken, men at lenken gjøres tilgjengelig på en nettside eller innfor en kontekst der man tjener penger på aktiviteten.

Den som skal tilby lenken innenfor en slik «profittkontekst» bør altså forsikre seg om at det aktuelle verket ikke er gjort tilgjengelig på en ulovlig måte. Kravet til denne forundersøkelsen kunne nok vært uttalt på en enklere måte. Det som reelt legges til grunn er en presumsjon for at den profesjonelle part har den kunnskap som måtte følge av en slik undersøkelse. Hvorvidt det rent faktisk er gjort noen slik undersøkelse vil dermed ikke være avgjørende i seg selv. Dette gjelder altså *«forudsat at denne afkræftelige formodning ikke afkræftes»*, som mer enn antyder at vi kan få diskusjoner i fremtiden på hva som ligger i kravet til denne *formodningen* eller kunnskapspresumsjonen.

Denne prejudisielle avgjørelsen følger altså opp tidligere praksis fra EU-domstolen knyttet til lenking på Internett, men videreutvikler læren med utgangspunkt i de konkrete omstendighetene i denne saken. Med bakgrunn i at GeenStijl hadde positiv kunnskap om manglende samtykke fra rettighetshaverne allerede før første publisering, artikkelens innhold som viste til lekkede bilder og de etterfølgende artikler med nye lenker lå saken godt an for en vurdering knyttet opp mot lenkerens subjektive forhold. Dette gjør det enklere å forstå hvorfor EU-domstolen trekker frem en individualiserende metode for å løse spørsmålene som lå til vurdering. På samme måte gjør dette det lettere å forstå kritikk som går på at domstolene med dette har gjort et allerede vanskelig spørsmål mer komplisert. Det er ikke vanskelig å se for seg en rekke scenarioer der grensene for lovlig og ulovlig lenking vil være vanskelig å trekke.

Samtidig skal vi ikke miste av syne at domstolen har gitt anvisning på de momentene som er relevante for vurderingen og hvordan disse forholder seg til hverandre. Min vurdering er at kriteriet knyttet til profitt sammenholdt med kunnskapspresumsjonen vil medføre de største utfordringene fremover. Jeg tenker da ikke bare på saker som kommer inn til rettsapparatet og som vi møter i form av dommer og avgjørelser fremover. Jeg tenker mer på bloggere, instagrammere, twitrere, snappere, forumskribenter og nettaviser som skal lenke til eksternt innhold og som har et profittelement ved seg. Disse forventes nå å gjøre seg opp en mening om hva som er lovlig publisert innhold med rettighetshavers samtykke.

Det er ikke til å unngå at denne avgjørelsen vil gi grunnlag for diskusjon knyttet til sensur av lenker ved at rettighetshavere potensielt kan få et for effektivt vern. EU-domstolen viser da også i denne og andre avgjørelser til det strenge vernet som er forutsatt i InfoSoc-direktivets artikkel 3 første ledd, og legger dette til grunn i sine betraktninger. På denne bakgrunn er det viktig å fremheve at EU-domstolen konkret fremhever nettopp hensynet til ytrings- og informasjonsfriheten, og at dette vil måtte være et fremtredende hensyn som skal vektlegges i den konkrete vurdering, ref. avsnitt 45:

«I denne henseende må det konstateres, at internettet er særligt vigtigt for ytrings- og informationsfriheden, som er sikret ved chartrets artikel 11, og at hyperlinks medvirker til, at internettet er velfungerende og til udveksling af meninger og information på dette netværk, der er karakteriseret ved adgang til uanede mængder af information.»

I denne avgjørelsen ligger det uansett en sterk oppfordring for kommersielle aktører til faktisk å oppsøke verket det lenkes til og gjøre seg kjent med rammen og konteksten for tilgjengeliggjøringen, så vil kunnskapsvurderingen langt på vei måtte avgjøres på bakgrunn av god lenkeskikk, sammenholdt med rettighetshaverens berettigede forventning om vern.

Gorrissen Federspiel

Janne Glæsel

Storbritannien omfattes i første omgang af den nye persondataforordning

Den britiske premierminister, Theresa May, offentliggjorde den 2. oktober 2016, at Storbritannien vil benytte sig af artikel 50 i Traktaten om Den Europæiske Unions Funktionsmåde (TEUF) inden udgangen af marts 2017. Artikel 50 i TEUF vedrører en medlemsstats frivillige udtræden af EU, og bestemmelsen udgør den eneste juridiske mekanisme for en sådan udtræden. Hvis Storbritannien vil benytte sig af artikel 50 i TEUF, skal den britiske regering underrette Det Europæiske Råd gennem en mundtlig eller skriftlig beslutning. Herefter vil processen for Storbritanniens ophør med at være medlem af EU formelt blive sat i gang. Denne proces vil tage mindst to år at gennemføre, og det betyder, at forordning (EU) 2016/679 (generel forordning om databeskyttelse) når at blive en del af britisk ret i omegnen af et års tid. Det fremgår af artikel 50, stk. 2 i TEUF, at EU vil indgå en aftale med Storbritannien om de nærmere bestemmelser for statens udtræden under hensyn til rammen af landets fremtidige forbindelser med EU. Det er dog stadig uklart, hvilken databeskyttelseslovgivning Storbritannien vil gøre gældende efter landets udtræden af EU.

Læs mere om processen her:
http://www.instituteforgovernment.org.uk/brexit/brexit-brief-article-50

Læs mere her:
http://www.clydeco.com/insight/article/global-data-privacy-update-october-2016

Microsoft kunne ikke tvinges til at overgive e-mails, der var lagret på servere uden for USA

Den amerikanske appeldomstol på Manhattan afsagde den 14. juli 2016 dom i en sag mellem Microsoft og den amerikanske stat. Sagen omhandlede den amerikanske stats adgang til at påbyde Microsoft at overgive e-mails fra deres kunder uden for USA til de amerikanske myndigheder. I sagen befandt de omhandlede e-mails sig på servere i et af Microsofts datacentre i Irland.

Den amerikanske byret på Manhattan besluttede i 2014, at Microsoft skulle overgive de omhandlede e-mails på baggrund af en ransagningskendelse udstedt af de amerikanske myndigheder. Appeldomstolen kom imidlertid frem til det modsatte resultat. Ifølge denne kunne ransagningskendelsen ikke finde anvendelse på data, der befinder sig uden for USA. Microsoft fik således medhold i sagen og kunne derfor ikke tvinges til at overgive de e-mails, som var lagret på virksomhedens servere uden for USA.

Læs hele dommen her:
https://www.justsecurity.org/wp-content/uploads/2016/07/Microsoft-Ireland-2d-Cir-Opinion-20160714.pdf

EU

Europa Parlamentet og Rådet vedtager direktiv om net- og informationssystemer

Europa Parlamentet og Rådet vedtog den 6. juli 2016 direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen. Direktivet trådte i kraft den 8. august 2016.

Direktivet skal øge sikkerhedsniveauet for net- og informationssystemer ved, at EU-medlemsstaterne blandt andet: 1) vedtager en national strategi for sikkerhed i net- og informationssystemer, 2) udpeger en eller flere kompetente nationale myndigheder til at varetage sikkerheden i net- og informationssystemer, 3) udpeger en eller flere enheder (CSIRT'er) til at håndtere IT-sikkerhedshændelser og risici i overensstemmelse med en nærmere fastlagt proces, og 4) sikrer, at operatører inden for væsentlige tjenester og udbydere af digitale tjenester lever op til en række sikkerhedskrav og foretager underretninger om visse hændelser.

I henhold til direktivet skal der oprettes en samarbejdsgruppe, der har til formål at støtte og lette samarbejdet og udvekslingen af oplysninger mellem EU-medlemsstaterne gennem tillid og gennem et højt fælles sikkerhedsniveau i net- og informationssystemer.

Læs direktivet her:
http://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:32016L1148&from=EN

EU-domstolen

Behandling af personoplysninger skal opfylde databeskyttelseslovgivningen i de medlemslande, som en virksomheds aktivitet tager sigte på

EU-Domstolen besvarede en præjudiciel forespørgsel den 28. juli 2016 i sag C-191/15. Sagen rejste blandt andet spørgsmål om, hvilken lovgiv-

ning, der regulerer en virksomheds behandling af personoplysninger, når behandlingen sker som led i udøvelse af virksomhed i andre medlemslande end det, hvor virksomheden har hjemsted.

Amazon EU med hjemsted i Luxembourg havde indgået elektroniske salgskontrakter med forbrugere bosiddende i Østrig. I Østrig blev der anlagt en sag med påstand om forbud mod anvendelse af vilkårene i salgskontrakternes almindelige forretningsbetingelser. Af forretningsbetingelserne fremgik blandt andet vilkår om behandling af personoplysninger.

EU-Domstolen fandt, at behandling af personoplysninger skal reguleres af loven i det medlemsland, som virksomhedens aktiviteter tager sigte på. Det er en betingelse, at virksomheden behandler de pågældende oplysninger som led i udøvelsen af dens virksomhed på medlemslandets område. EU-Domstolen henviste til eksisterende praksis på området og udtalte, at udøvelse af virksomhed omfatter enhver reel og faktisk aktivitet, der udøves gennem en permanent struktur. Det er ikke afgørende, om den dataansvarlige virksomhed har et datterselskab eller en filial i det pågældende medlemsland.
EU-Domstolen mener, at der i højere grad bør foretages en vurdering af, i hvilken grad strukturen er permanent, og om der faktisk udøves aktiviteter i det pågældende medlemsland. EU-Domstolen udtalte også, at det ved vurderingen af, om behandlingen er foretaget som led i virksomhedens aktiviteter, ikke er afgørende, om behandlingen er foretaget direkte af virksomheden. Behandling som led i virksomhedens aktiviteter er også tilstrækkelig.
EU-Domstolen henviste sagen tilbage til den nationale østrigske ret, der skal anvende domstolens afgørelse som vejledning til endelig afgørelse i sagen.

Læs den præjudicielle forelæggelse her:
http://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX%3A62015CJ0191&from=DA

Privacy Shield

EU-Kommissionen vedtager EU-U.S. Privacy Shield-aftalen

Vi har tidligere beskrevet at EU og USA har underskrevet EU-U.S. Privacy Shield-aftalen, og den 12. juli 2016 blev den endelige tekst til EU-U.S. Privacy Shield-aftalen endeligt vedtaget af EU-Kommissionen. Aftalen, der udgør et værn om privatlivets fred, har til formål at agere som overførselsgrundlag ved overførsler mellem virksomheder i EU og virksomheder i USA, der har ladet sig certificere under EU-U.S. Privacy Shield-aftalen.

Amerikanske virksomheder har siden 1. august 2016 kunnet tilslutte sig den nye EU-U.S. Privacy Shield-aftale gennem det amerikanske Handelsdepartements hjemmeside. Virksomhederne, der tilslutter sig aftalen, forpligter sig til at følge de særlige persondatabeskyttelsesforanstaltninger, som aftalen medfører. Ifølge aftalen vil virksomhederne skulle overholde et sæt af regler når de behandler persondata (se nærmere i artiklen nedenfor) og vil samtidig være underlagt ajourføring og kontrol, der foretages af USA's handelsministerium. Ved manglende overholdelse af kravene i aftalen, kan virksomhederne risikere sanktioner og fjernelse fra ordningen. I sidstnævnte tilfælde skal virksomhederne tilbagelevere eller slette persondata, som virksomheden har modtaget under EU-U.S. Privacy Shield-aftalen.

USA har i forbindelse med aftalen givet EU garanti for, at den amerikanske stats adgang til personoplysninger er undergivet klare begrænsninger, beskyttelsesforanstaltninger og tilsyn.

Læs pressemeddelelsen her:
http://europa.eu/rapid/press-release_IP-16-2461_en.htm

Læs aftalen her:
http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf

Amerikanske virksomheder kan tilslutte sig ordningen her:
https://www.privacyshield.gov/PrivacyShield/ApplyNow

EU-Kommissionen udgiver vejledning om EU-U.S. Privacy Shield-aftalen

EU-Kommissionen udgav den 1. august 2016 en vejledning om EU-U.S. Privacy Shield-aftalen. Formålet med vejledningen er blandt andet at redegøre nærmere for virksomhedernes forpligtelser, EU-borgernes rettigheder, klageadgangen ved overtrædelser og ombudsmandsmekanismen.

Virksomhederne er som følge af aftalen forpligtet til at beskytte EU-borgernes data. Ifølge vejledningen skal dette ske ved at sikre: 1) EU-borgernes ret til information, 2) begrænsninger i brugen af data til andre formål end det oprindeligt tiltænkte, 3) databegrænsning, således at mængden og opbevaringstiden af data begrænses til det højst nødvendige, 4) at virksomheden beskytter EU-borgernes data, herunder også ved overførsel

til andre virksomheder, 5) at andre virksomheder (sub-databehandlere) overholder kravene i EU-U.S. Privacy Shield-aftalen, 6) EU-borgeres adgang til og berigtigelse af data, 7) retten til klageadgang og udnyttelse af misligholdelsesbeføjelser, og 8) afhjælpning gennem ombudsmandsmekanismen.
Vejledningen omfatter også retningslinjer for, hvordan der kan indgives klager over de virksomheder, der deltager i ordningen og de amerikanske myndigheder. Vedrører klagen virksomhederne, kan EU-borgerne vælge mellem forskellige tvistløsningsmekanismer. Vedrører klagen en offentlig amerikansk myndighed, skal ombudsmandsmekanismen tages i brug.

Læs EU-Kommissionens vejledning her:
http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf

Digital Rights Ireland anlægger sag om annullation af Privacy Shield-afgørelsen

Den 16. september 2016 anlagde den irske privatlivsgruppe Digital Rights Ireland sag an mod EU-Kommissionen ved EU-domstolen, i sag T-670/16, der skal udfordre EU-Kommissionens EU-U.S. Privacy Shield-afgørelse.
EU-U.S. Privacy Shield-aftalen blev indgået som afløser til Safe Habour-ordningen, som EU-Domstolen ugyldiggjorde med sin afgørelse i den såkaldte Schrems afgørelse (C-362/14). På nuværende tidspunkt er det blot blevet offentliggjort, at sagen vedrører et annullationssøgsmål, men de nærmere detaljer herfor er endnu ikke offentliggjort. Digital Rights Ireland har ved annullationssøgsmålet dermed benyttet sig af sig af retten til at udfordre EU-reguleringer, som tilkommer enkeltpersoner og virksomheder, der er direkte berørt af reguleringens ikrafttræden.

Læs mere her:
http://www.reuters.com/article/us-eu-dataprotection-usa-idUSKCN12Q2JK

Artikkel 29-gruppen

Artikel 29-gruppen udtaler sig om E-databeskyttelsesdirektivet

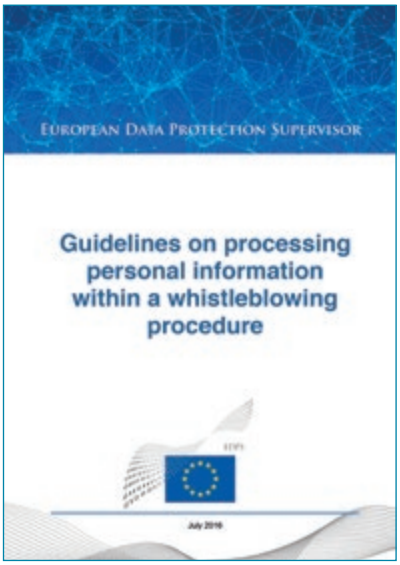
Artikel 29-gruppen offentliggjorde den 19. juli 2016 en udtalelse om direktiv 2002/58/EF (E-databeskyttelsesdirektivet). Artikel 29-gruppen støtter EU-Kommissionens anerkendelse af behovet for specifikke regler for elektronisk kommunikation i EU.

Artikel 29-gruppen anbefalede blandt andet: 1) at direktivets rækkevidde bør udvides til at omfatte nye OTT tjenesteudbydere, 2) at definitionerne bør genovervejes, 3) at offentligt tilgængelige private kommunikationsnetværker bør være omfattet, 4) at EU-Kommissionen eksplicit anfører, at der ikke indføres nye europæiske krav for opbevaring af data, 5) at fortroligheden af elektronisk kommunikation i højere grad bør varetages, og at dette kan ske ved en række ændringer i E-databeskyttelsesdirektivet, 6) at der fortsat bør være fokus på brugernes samtykke, 7) at artikel 4.2 og 4.3 i E-databeskyttelsesdirektivet om databrud bør fjernes, 8) at der bør foretages en harmonisering af de bestemmelser, der vedrører uopfordret kommunikation og registre over abonnenter, 9) at der tages højde for Call Line Identification, og 10) at EU-Kommissionen angiver, at de nationale databeskyttelsesmyndigheder har kompetence til håndhævelse af det nye E-databeskyttelsesregelsæt.

Læs udtalelsen her:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf

EDPS

EDPS udgiver vejledning om behandling af personoplysninger inden for whistleblower-ordningen



Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) udgav i juli 2016 en vejledning om, hvordan EU-institutionerne- og organerne kan overholde databeskyttelsesreglerne i forordning (EF) nr. 45/2001 (generel forordning om databeskyttelse) både før og efter implementeringen af en whistleblower-ordning. EDPS har udstedt ni anbefalinger, som også fungerer som tjekliste, når EDPS vurderer, om forpligtelserne i forordningen er overholdt.

EDPS vil i den forbindelse undersøge: 1) om der er etableret ka-

naler for intern og ekstern rapportering, og om der er særlige regler, hvor formålet klart fremgår, 2) om fortroligheden af den modtagne information er sikret, og om identiteten på whistlebloweren og andre involverede personer er beskyttet, 3) om behandlingen af persondata er proportional, relevant og nødvendig, 4) om der i det enkelte tilfælde er tale om persondata, om de berørte personer er identificeret, og om deres ret til information, adgang og berigtigelse af data er fastslået, 5) om to trins-proceduren er anvendt til at informere grupperne af berørte individer om, hvordan deres data bliver behandlet, 6) om andres persondata er videregivet ved anmodninger herom, 7) om der er taget stilling til kompetencen hos modtageren af persondata, og om dataoverførslerne er begrænset i nødvendigt omfang, 8) om opbevaringsperioden for persondata er proportional med whistleblower-ordningens formål, og 9) om der er gennemført organisatoriske og tekniske sikkerhedsforanstaltninger baseret på en risikovurdering, der sikrer at whistleblower-ordningen indebærer lovlig og sikker databehandling.

Læs vejledningen her:
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/16-07-18_Whistleblowing_Guidelines_EN.pdf

EDPS udtaler sig om databeskyttelse under E-databeskyttelsesdirektivet

Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) udtalte sig den 22. juli 2016 om problemerne forbundet med direktiv 2002/58/EF (E-databeskyttelsesdirektivet) i forbindelse med databeskyttelse inden for elektronisk kommunikation. Ifølge EDPS er der behov for smartere, klarere og stærkere regulering på området.

EDPS udtalte, at der ved reguleringen af databeskyttelse inden for elektronisk kommunikation er behov for: 1) mere klarhed, 2) forbedret håndhævelse, 3) sikring af fortrolighed ved kommunikation, 4) bestemmelser, der supplerer og på nødvendige områder præciserer beskyttelsen under forordning (EU) 2016/679 (den generelle databeskyttelsesforordning), og 5) en højere grad af beskyttelse på de områder, hvor direktivet om databeskyttelse inden for elektronisk kommunikation giver bedre beskyttelse end den generelle databeskyttelsesforordning.

EDPS udtalte også, at der er behov for en udvidelse af reguleringens rækkevidde. Ifølge EDPS bør der tages hensyn til teknologiske og samfundsmæssige ændringer, og det bør sikres, at alle individer opnår den samme beskyttelse ved både funktionelt tilsvarende tjenester og tjenester, der tilbyder nye muligheder for kommunikation. Derudover udtalte EDPS, at det nye regelsæt entydigt bør dække kommunikation fra maskine til maskine, uanset netværkstypen eller kommunikationstjenesten, og bør sikre fortrolighed ved brugernes kommunikation på alle offentligt tilgængelige netværker.

EDPS udtalte sig også om samtykke, kryptering og uønsket kommunikation.

Læs udtalelsen her:
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-07-22_Opinion_ePrivacy_EN.pdf

EDPS udtaler sig om oprettelsen af og formålet med »Digital Clearing House«

»The European Data Protection Supervisior« (EDPS) udtalte den 23. september 2016, at problemerne ved den øgede konkurrence om personoplysninger på de digitale markeder og den begrænsede hensynstagen til det enkelte individ kan løses ved oprettelse af et »Digital Clearing House«, der forestår håndhævelse i den digitale sektor i EU.

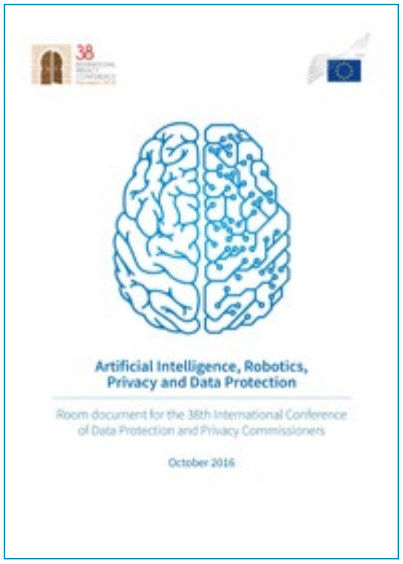
»Digital Clearing Houses« vil bestå af et netværk af tilsynsorganer, der opererer inden for rammerne af deres tildelte kompetenceområder. Tilsynsorganerne skal frivilligt dele oplysninger om eventuelt misbrug i det digitale økosystem og vejlede om, hvordan sådan misbrug tackles på den mest effektive måde. Ordningen har blandt andet til formål at fremme en sammenhængende håndhævelse af EU's persondataretlige regler.

Udover etableringen af »Digital Clearing Houses« vedrørte udtalelsen: 1) at der skulle udarbejdes en vejledning om, hvordan lovgiver kan tage hensyn til reglerne om beskyttelse af personoplysninger, 2) en anbefaling om, at EU-institutionerne benytter eksterne eksperter til at undersøge etableringen af et fælles område på internettet, som er i overensstemmelse med EU-retten, og hvor interaktionen ikke kan blive sporet, og 3) en opdatering af reglerne for, hvordan myndighederne bedre kan beskytte personoplysninger og ytringsfriheden.

EDPS foreslog derudover, at myndighederne bør arbejde tættere sammen for en øget beskyttelse af individets rettigheder, herunder retten til privatlivets fred, ytringsfriheden og retten til ikke at blive diskrimineret.

Læs hele udtalelsen her:
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Events/16-09-23_BigData_opinion_EN.pdf

EDPS udtaler sig om kunstig intelligens, robotteknologi, privatlivs- og databeskyttelse



»The European Data Protection Supervisior« (EDPS) udgav den 19. oktober 2016 en rapport i anledning af den 38. International Conference of Data Protection and Privacy Commisioners. Rapporten omhandler kunstig intelligens, robotteknologi, privatlivs- og databeskyttelse.

EDPS udtalte, at kunstig intelligens og robotteknologi er en stigende realitet, der er fremtrædende på den politiske agenda. På denne baggrund er der behov for en realistisk tilgang til området, og ifølge EDPS bør der findes et forsvarligt grundlag for udvikling, der ikke hæmmer innovation på området.

Rapporten reflekterer over en række populære områder, inden for kunstig intelligens og robotteknologi, som giver anledning til at diskutere, hvorvidt privatlivs- og databeskyttelse påvirkes. De omdiskuterede områder er: Big Data, profilering, automatisk beslutningstagning, billedgenkendelse, sprogteknologi, autonome maskiner, selvkørende biler og droner.

EDPS fremhæver blandt andet, at det er nødvendigt at tage stilling til både etiske og tekniske aspekter ved de omtalte teknologier. Teknologierne bør hverken diktere samfundets værdier og rettigheder, samfundsmæssige interaktioner eller strukturer. Ifølge EDPS er der således behov for at udvikle og fremme teknikker og metoder, der gør teknologierne i stand til at respektere individets rettigheder og værdighed.

Læs hele rapporten her:
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/16-10-19_Marrakesh_AI_paper_EN.pdf

Forbrugerombudsmanden

De nordiske forbrugerombudsmænd styrker samarbejdet med fokus på dataindsamling

Den danske forbrugerombudsmand (Forbrugerombudsmanden) udtalte den 14. oktober 2016, at hun sammen med forbrugerombudsmændene i Norge, Sverige og Finland vil styrke samarbejdet om de udfordringer, der knytter sig til den digitale udvikling i forhold til data-, privatlivs- og forbrugerbeskyttelse.

Ifølge Forbrugerombudsmanden medfører den digitale udvikling, at virksomhederne får nye redskaber til at anvende forbrugernes personlige oplysninger til markedsføring. Forbrugerbeskyttelsen er klar på visse områder, men som følge af den teknologiske udvikling bliver virksomhedernes anvendelse af data mere kompleks, og forbrugerne står derfor over for nye udfordringer.

Forbrugerombudsmanden udtalte, at det er positivt med et nordisk samarbejde, fordi udfordringerne i de nordiske lande minder om hinanden. Det forventes således, at forbrugerombudsmændene kan få gavn af samarbejdet, da det kan danne grundlag for deling af sammenlignelige erfaringer.

Læs udtalelsen her:
http://www.forbrugerombudsmanden.dk/Nyheder-fra-FO/Pressemeddelelser/2016/De-nordiske-forbrugerombudsmaend-oeger-fokus-paa-dataindsamling?tc=D74929A5CD4D4F43909476CBFC7C9FE1

Datatilsynet

Datatilsynet indfører ny anmeldelsesprocedure for alle lovpligtige whistleblowerordninger

Det danske datatilsyn (Datatilsynet) udtalte den 14. oktober 2016, at det har valgt at indføre en ny anmeldelsesprocedure for lovpligtige whistleblowerordninger. Proceduren er indført på baggrund af et sæt nye regler, der træder i kraft den 1. januar 2017. Reglerne stiller krav om, at erhvervsvirksomheder opretter særlige whistleblowerordninger. Under disse ordninger vil det fremadrettet være muligt for virksomhedernes ansatte at foretage anonyme indberetninger af overtrædelser eller potentielle overtrædelser af særlovgivningen.

Datatilsynet har som følge af de nye regler bestemt, at enhver ordning kan anmeldes ved brug af en ny blanket: WB1 (whistleblowerordning, hvor den dataansvarlige virksomhed er etableret i Danmark). Denne blanket skal både anvendes ved anmeldelsen af frivillige whistleblowerordninger og ved lovpligtige ordninger. Ændringen medfører

Illustrasjon: Luth

fremadrettet, at den tidligere blanket til standardanmeldelse, FWB (whistleblowerordning på det finansielle område), er afskaffet. Efter den nye anmeldelsesprocedure skal således også de finansielle virksomheders lovpligtige whistleblowerordninger anmeldes ved brug af den nye blanket WB1.

Læs udtalelsen her:
https://www.datatilsynet.dk/nyheder/nyhed/artikel/ny-anmeldelsesprocedure-for-lovpligtige-whistleblowerordninger/

Datatilsynet udgiver ny it-sikkerhedstekst om fælles login
Det danske datatilsyn (Datatilsynet) udgav den 26. oktober 2016 en it-sikkerhedstekst (ST11) vedrørende fælles login. Teksten beskriver, hvilke udfordringer der kan være forbundet med fælles login og giver i den forbindelse råd til, hvordan udfordringerne kan håndteres. Derudover indeholder teksten eksempler på, hvad der bør indgå i overvejelserne, når det skal vurderes, om fælles login er forsvarligt.

Ifølge it-sikkerhedsteksten bør følgende forhold indgå i overvejelserne: 1) brugernes ansvarsfølelse, 2) begrænsning af dataadgang via fælles login, 3) fysisk og tidsmæssig begrænsning, 4) restriktioners afledte effekt, 5) periodisk kontrol af adgang til it-systemer, 6) den adgangsgivende faktors styrke, 7) skift eller inddragelse af den adgangsgivende faktor, 8) genudstedelse af faktor og 9) administration af brugere og faktor.

Læs it-sikkerhedsteksten her:
https://www.datatilsynet.dk/fileadmin/user_upload/ST11_Faelles_login.pdf

Dansk Højesteret

Højesteret tilkendte ikke medarbejdere godtgørelse i sag, hvor persondataloven var overtrådt
Den danske højesteret (Højesteret) afsagde den 29. september 2016 dom i sagen 277/2015. Sagen angik, hvorvidt Banedanmarks håndtering af tre ansattes lægeerklæringer var lovstridig. De tre ansatte var alle blevet afskediget fra Banedanmark efter sygemelding i en længere periode, og Banedanmark havde i forbindelse med afskedigelserne indhentet helbredsoplysninger.

Den danske Østre Landsret (Østre Landsret) havde den 8. december 2015 afsagt dom i sagen. Ifølge Østre Landsret var der blandt andet sket en overtrædelse af lov nr. 429 af 31. maj 2000 (den danske persondatalov) i forhold til to af medarbejderne. Retten kom dog frem til, at overtrædelsen ikke berettigede til tortgodtgørelse efter § 26, stk. 1 i lovbekendtgørelse nr. 266 af 21. marts 2014 (den danske erstatningsansvarslov). Dette var henset til, at oplysningerne ikke var tilgået en bredere kreds af personer, og at håndteringen af oplysningerne ikke havde påvirket den materielle rigtighed af personalesagernes udfald.

Højesteret stadfæstede Østre Landsrets dom. Højesteret valgte således, lige som landsretten, at undlade at tilkende de to ansatte tortgodtgørelse, selvom der forelå et brud på den danske persondatalov.

Læs Østre Landsrets dom her:
http://domstol.fe1.tangora.com/media/-300016/files/277-2015-ØL.pdf

Læs Højesterets dom her:
http://domstol.fe1.tangora.com/media/-300016/files/277-2015.pdf

Janne Glæsel er partner i advokatfirmaet Gorrissen Federspiel og er en av de danske redaktørene i Lov&Data.



Delphi
Henrik Bengtsson
Frida Solding
Caroline Sundberg

Principiell dom rörande tolkningen av personuppgiftsbegreppet från EU-domstolen

Den 19 oktober 2016 meddelade EU-domstolen förhandsbesked i ett mål mellan Patrick Breyer och Förbundsrepubliken Tyskland (mål nr C-582/14). Breyer hade väckt talan vid tysk förvaltningsdomstol och yrkade att Tyskland skulle förbjudas att lagra eller uppdra åt tredje man att lagra Patrick Breyers IP-adresser när han hade besökt de tyska myndigheternas webbplatser.

Tyska Bundesgerichtshof frågade i sammanfattning EU-domstolen huruvida personuppgiftsbegreppet i 2 a i dataskyddsdirektivet skulle tolkas så, att en IP-adress som en ISP registrerar i samband med att någon använder dennes webbplats utgör en personuppgift för denne även om det är abonnentens ISP som har tillgång till den ytterligare information som behövs för att identifiera abonnenten?

Frågan huruvida IP-nummer utgör en indirekt personuppgift har i Sverige prövats av Kammarrätten i Stockholm (mål nr 285-08) som ansåg att ett IP-nummer var en personuppgift hos tredje part trots att det endast var ISP:n som kunde identifiera abonnenten med hjälp av IP-nummer. Datainspektionen har i bl a ärende dnr 811-2011 bedömt huruvida krypterade personuppgifter i forskningsmaterial där den som behandlade informationen inte kunde identifiera de registrerade men där det hos en tredje man fanns en nyckel som möjliggjorde bakvägsidentifikation utgör personuppgifter. Datainspektionens bedömning var att eftersom bakvägsidentifikation var möjlig var uppgifterna personuppgifter. Datainspektionen har haft samma synsätt när det gäller reseuppgifter (dnr 857-2005, 183-2007, 550-2007 och 1356-2007) och ofullständiga kontokortsnummer (dnr 705-2009) där den personuppgiftsansvarige inte kunnat göra identifikationen men det funnits en ”nyckel” att identifiera den registrerade hos tredje part.

Frågan huruvida en indirekt personuppgift är en personuppgift i dataskyddsdirektivets (direktiv 95/46/EG) mening är praktiskt väsentlig eftersom det avgör om personuppgiftslagen (PUL) alls är tillämplig på en behandling. Tolkningen får också betydelse för huruvida etikprövningslagen är tillämplig på personuppgiftsbehandling i samband med klinisk forskning.

Flera medlemsstater, däribland Storbritannien och Irland tillämpar ett relativt personuppgiftsbegrepp vilket innebär att en uppgift utgör en personuppgift endast om den registrerade kan identifieras utifrån den information som den personuppgiftsansvarige har tillgång till eller sannolikt kan få tillgång till, vilket är en snävare syn på indirekta personuppgifter än den svenska synen. EU-domstolens dom är därför välkommen eftersom den kan harmoniera personuppgiftsbegreppet inom EU.

I Breyer-domen konstaterar EU-domstolen det först behöver fastställas huruvida möjligheten att kombinera en dynamisk IP-adress med den information som ISP:n innehar utgör ett hjälpmedel som rimligen kan komma att användas för att identifiera abonnenten (domskäl 45). Om identifiering av abonnenten är förbjuden i lag eller omöjlig att genomföra i praktiken, exempelvis på grund av att den skulle kräva orimliga resurser i form av tid, kostnader och arbetskraft, med den följden att risken för identifiering i praktiken var försumbar är uppgiften inte en personuppgift (domskäl 46).

Om det däremot finns lagliga medel för den som behandlar IP-numret att vända sig mot ISP:n som gör det möjligt för vederbörande att identifiera den registrerade med hjälp av den information som ISP:n förfogar över utgöruppgiften en personuppgift (domskäl 47-49). EU-domstolen tycks utgå från att det är tillräckligt att det finns en laglig möjlighet att vända sig mot ISP:n men att denna inte behöver ha utnyttjats. Frågan om det finns lagliga medel att hos tredje part komma åt ”nycklar” till andra uppgifter är en fråga för de enskilda medlemsstaternas process- och sekretessregler. Frågan om vad som är en personuppgift kan därmed få helt olika utfall i olika medlemsstater vilket knappast kan anses ha bidragit till harmoniseringen.

Breyer-domens betydelse för det svenska personuppgiftsbegreppet – finns det lagliga medel för den personuppgiftsansvarige att få del av ”nyckeln”?

När det gäller IP-nummer får enligt svensk rätt en ISP enligt 6 kap 16 a) § LEK (lagen om elektronisk kommunikation) inte lämna ut abon-

nentuppgifter såsom vem som innehaft en IP-adress vid en viss tidpunkt till tredje part om uppgifterna sparats för brottsbekämpningsändamål till andra än brottsbekämpande myndigheter. Däremot kan en ISP enligt 6 kap 20 a) § LEK lämna ut abonnentuppgifter som ISP:n sparat ex vis för fakturerings- eller säkerhetsändamål om en domstol meddelar ett beslut om edition eller informationsföreläggande mot ISP:n eftersom ett sådant beslut genombryter sekretessen (se NJA 2012 s. 975). Ett IP-nummer utgör därmed enligt svensk rätt sannolikt en personuppgift om ISP:n sparat abonnentinformation för annat än brottsbekämpningsändamål eftersom det i en sådan situation finns en laglig möjlighet för den som behandlat IP-numret att få del av abonnentinformationen. Har ISP:n inte sparat sådan information utgör IP-numret inte en personuppgift hos den tredje part som behandlar IP-numret. Ett problem i sammanhanget är att det endast är ISP:n som vet huruvida informationen behandlas för andra ändamål är brottsbekämpning vilket innebär att tredje part inte kan veta huruvida det finns lagliga möjligheter att komma åt informationen och huruvida IP-numret därmed utgör en personuppgift.

> Indirekta personuppgifter såsom patientdata, kontonummer eller reseinformation bör i det stora flertalet fall inte längre anses utgöra personuppgifter.

Även när det gäller andra indirekta personuppgifter uppstår frågan om det finns en laglig möjlighet för den som behandlar uppgiften att få del av den kompletterande information från tredje part för att kunna knyta informationen till en person. Ytterst blir detta en fråga om i vilken utsträckning nationella processrättsliga regler om edition, informationsföreläggande och vittnesförhör kan genombryta lagreglerad sekretess hos den part som innehar ”nyckeln” som medför att en viss uppgift kommer att utgöra en personuppgift. Av Högsta domstolens dom i NJA 2012 s. 975, följer att om den lagreglerade sekretessbestämmelsen innebär att sekretessbelagd information inte obehörigen får lämnas ut till en sökande avseende informationsföreläggande eller edition bryter ett domstolsbeslut igenom sekretesskyddet eftersom utlämnandet blir behörigt. Detsamma har ansetts gälla när det gäller banksekretessen (se Rättsfall från Hovrätterna RH 1997:46). I RH 1999:97 har Göta hovrätt däremot uttalat att rättegångsbalkens regler om bl a edition inte skall bryta skyddet för telemeddelanden eftersom den dåvarande telelagen uttömmande reglerade frågan om när information kunde lämnas ut. Frågan om när edition kan bryta lagreglerad sekretess förefaller därmed vara oklar. HD:s avgörande i NJA 2012 s. 975 är dock tydligt vad som gäller när sekretessen enbart skyddar mot obehöriga utlämnanden såsom i LEK.

Frågan huruvida det finns en laglig möjlighet att komma åt ”nyckeln” kompliceras av att en editionssökande enligt den svenska rättegångsbalken endast kan begära edition inom ramen för en pågående rättegång och att domstolen endast bifaller en editionsansökan om uppgifterna är preciserade och relevanta liksom att det finns ett bevistema för den editionssökta informationen. I det stora flertalet situationer där en innehavare av en uppgift skulle kunna ha ett intresse av att få del av nyckeln hos tredje man kommer dessa lagliga medel i praktiken inte vara tillgängliga eftersom det antingen inte pågår någon rättegång eller en domstol skulle ogilla editionsansökan på grund av att informationen saknar relevans för tvisten. När det gäller IP-nummer och upphovsrättsintrång kan dock bedömningen bli en annan beroende på vilken IP-nummerinformation ISP:n sparat.

Slutsatsen av det ovan sagda – för svensk rätts vidkommande – är att det i de flesta fall som det finns teoretiska lagliga medel för att komma åt en ”nyckel” för att identifiera en personuppgift är det omöjligt att genomföra i praktiken. Detta leder till att indirekta personuppgifter såsom patientdata, kontonummer eller reseinformation i det stora flertalet fall inte bör anses utgöra personuppgifter. Detta innebär en tydlig förändring i förhållande till den nu gällande svenska synen på indirekta personuppgifter som måste anses mycket vidsträckt eftersom det faktum att den personuppgiftsansvarige är helt förhindrad att komma över ”nyckeln” hos tredje part inte har beaktats vid bedömningen.

EU-domstolens tolkning avser artikel 2 a) dataskyddsdirektivet (95/46/EG). Personuppgiftsbegreppet i artikel 4 (1) i dataskyddsförordningen (förordning (EU) 2016/679) har fått en annan lydelse men avser alltjämt information som ”[…] indirekt kan identifieras särskilt med hänvisning till en identifierare […]. Beaktandesats 26 i förordningen som rör indirekta personuppgifter har stora likheter med beaktandesats 26 i dataskyddsdirektivet. Min tolkning är därför att den tolkning av personuppgiftsbegrepp som EU-domstolen har fastslagit i Breyer-domen kommer att gälla även enligt dataskyddsförordningen.

Henrik Bengtsson är partner i advokatfirman Delphi, Stockholm.

Ny vägledning från Datainspektionen rörande bedömning av integritetsrisker med ny eller ändrad lagstiftning

År 2010 ändrades den svenska grundlagen bland annat med syfte att säkerställa att de lagar som inskränker integritetsskyddet endast får genomföras om det intresse som ska tillgodoses är så starkt, och integritetsskyddsintresset är så förhållandevis svagt, att inskränkningen framstår som proportionerlig. Varje utredning måste därför göra en så kallad integritetsanalys. Integritetsanalysen ska belysa om föreslagna författningar medför någon form av personuppgiftsbehandling samt vilka konsekvenser detta i så fall innebär för den personliga integriteten.

För att en integritetsanalys ska uppfylla de krav som ställs räcker det inte med att slutsatsen redovisas i korthet, utan utredningen behöver noggrant beskriva den personuppgiftsbehandling som kan bli följden av utredningens förslag samt öppet redovisa de överväganden som gjorts rörande integritetsrisker.

I flera remissyttranden över lagförslag har Datainspektionen konstaterat att underlaget till betänkandet inte är tillräckligt utförligt för att det ska vara möjligt för inspektionen att ta ställning till de integritetsrisker som följer av förslaget. I syfte att underlätta arbetet med integritetsanalyser har Datainspektionen tagit fram en vägledning. Vägledningen är uppbyggd kring vissa centrala frågeställningar som kan behöva besvaras och redovisas i en integritetsanalys, samt förslag på åtgärder som kan vidtas för att minska integritetsrisker. De delar som tas upp rör bland annat automatiserad behandling av personuppgifter, personuppgiftsansvarig och insamling av personuppgifter.

I den nya dataskyddsförordningen (förordningen (EU) 2016/679), som ska börja tillämpas i maj 2018, finns det bestämmelser om konsekvensbedömning (artikel 35). Konsekvensbedömningen kan genomföras som ett led i lagstiftningsarbetet, och enligt Datainspektionen kan vägledningen i dessa fall användas som ett hjälpmedel vid genomförandet av en sådan bedömning.

Frida Solding är Associate vid Advokatfirman Delphi, Stockholm.

Avgöranden från Högsta förvaltningsdomstolen: Kamera på drönare omfattas av kameraövervakningslagen och tillstånd krävs för användning –kamera på bil och cykel är däremot undantagna från tillståndsplikten

Användningen av fjärrstyrda obemannade luftfarkoster, s.k. drönare, har blivit allt mer vanligt förekommande. Många drönare är utrustade med kamera och används t.ex. av mäklare, journalister eller landskapsarkitekter för att filma, fotografera och dokumentera från luften. Det har i Sverige rått delade meningar om drönare som är försedda med en kamera ska anses utgöra en övervakningskamera enligt kameraövervakningslagen (KÖL) eller inte. En övervakningskamera som omfattas av KÖL, som är riktad mot ett område dit allmänheten kan ha tillträde, kräver tillstånd från Länsstyrelsen. Länsstyrelsen är generellt sett restriktiv med att ge sådana tillstånd och har enligt praxis ofta nekat tillstånd om användning inte kan är nödvändig av säkerhetsskäl eller för att beivra återkommande brottslighet. Om ett tillstånd beviljas kan det villkoras av specificerade krav på vilken plats och under vilken tid på dygnet som användning är tillåten.

För att en kamerautrustning ska vara tillståndspliktig såsom övervakningskamera enligt KÖL krävs att den är uppsatt så att den, utan att manövreras på plats, kan användas för personövervakning. Detta innebär att placeringen av kameran ska ha en viss varaktighet, den ska kunna riktas mot platser dit allmänheten har tillträde och den ska kunna hanteras från en annan plats än där den är uppsatt.

Högsta förvaltningsdomstolen (HFD) har nu i två domar slagit fast att en kamera som är monterad på en drönare kräver tillstånd enligt KÖL medan en kamera som är monterad innanför vindrutan på en bil eller på ett cykelstyre inte behöver tillstånd.

I en dom den 21 oktober 2016 i mål nr 78-16 konstaterar HFD att även en kamera som fästs på ett rörligt objekt kan vara att anse som uppsatt på sådant sätt som KÖL förutsätter. En kamera som helt tillfälligt monteras på detta sätt kan dock knappast anses vara uppsatt. Det krävs att placeringen har en viss varaktighet för att kameran ska omfattas av KÖL:s tillämpningsområde. I det aktuella målet hade sökande anfört att kameran gick att

Bilde hentet fra https://pixabay.com/en/drone-espionage-camera-spy-nsa-407393/

plocka bort och enbart sattes dit för enskilda flygningar, något som HFD inte ansåg påverkade bedömningen eftersom det framgått att monteringen av kameran varit återkommande och bara det faktum att kameran kunde monteras bort inte fick någon betydelse i bedömningen.

När det avsåg bedömningen av om kamera skulle anses manövreras på plats (vilket om så är fallet gör att kameran inte faller in under KÖL), ansåg rätten bedömning bör göras utifrån om kameran kan anses fortlöpande hanteras från en plats som är klart åtskild från den där kameran är uppsatt. HFD fann vidare att eftersom fotograferingen med kameran sker i luften medan kameran och drönaren manövreras och i övrigt styrs från marken ska hanteringen anses ske från en plats som är klart åtskild från den där kameran är uppsatt och kameran kan därmed inte anses manövreras på platsen.

I bedömningen av om kameran kan anses vara uppsatt så att den ”kan användas för personövervakning” fastslog rätten att denna prövning ska göras utan att beakta vad som är det faktiska syftet med användningen och om kameran rent faktiskt används för personövervakning utan det avgörande är om den kan användas för sådan övervakning. Även om det i det aktuella fallet anfördes av sökande att denne pga. Transportstyrelsens föreskrifter är skyldig att hålla ett säkerhetsavstånd om minst 50 meter mellan drönaren och närmaste person och att kameran inte medger att enskilda personer identifieras på det avståndet har detta inte ha någon betydelse eftersom sökanden genom att styra drönaren kan styra denna så att den kan användas för personövervakning. Domstolen fann därmed att kameran på drönaren sammantaget ska anses vara sådan övervakningskamera som avses i KÖL.

I ett annat mål som avgjordes av HFD samma dag (21 oktober 2016 i mål nr 4110-15) som avsåg kamera uppsatt i en bil kom dock domstolen till en annan slutsats. I det aktuella målet prövades om en kamera som under färd är monterad på vindrutan i en bil eller på ett cykelstyre är en övervakningskamera. Med samma argumentation som i drönarmålet ansågs kameran vara varaktig uppsatt och betonade att detta gäller även om den monteras bort efter färd. I detta mål skulle dock kameran vara uppsatt på vindrutans insida i en bil eller på ett cykelstyre, dvs. i fordonsförarens omedelbara närhet. Eftersom föraren av cykeln eller bilen skulle starta och stänga av kameran samt kunde avgöra vad som ska filmas genom att styra fordonet ska manövrering av kameran anses ske på samma plats i detta fall. Genom att manövrering ska anses ske på samma plats fann HFD att aktuell kamera inte kan anses vara en övervakningskamera i KÖLs mening och något tillstånd därmed inte krävs för sådana kameror.

Sammantaget, även om ett antal detaljer och andra omständigheter skiljer åt i de båda avgjorda fallen verkar närheten till kameran (armlängds avstånd i bil och cykel och flertalet meter upp i luften i drönarfallet) samt om styrning av riktning görs i samma enhet som den som styr vara avgörande i prövningen av om tillståndsplikt föreligger.

I målet avseende drönare återförvisades prövningen av om tillstånd kan medges för den aktuella övervakningen tillbaka för vidare handläggning av förvaltningsrätten. Domen kan således inte ses som ett absolut förbud mot användning av kameror på drönare men mot bakgrund av den tidigare restriktiva praxis som finns för att medge sådana tillstånd får domen enligt vår bedömning stor betydelse för möjligheten att använda sådana kameror i den mån praxis inte förändras avseende när tillstånd ges.

Caroline Sundberg är advokat i Delphis ITC/IP-grupp och specialiserar sig inom IT och Internet-relaterad juridik. Hon biträder klienter vid många olika typer av juridiska frågor, inklusive outsourcing, IT-avtal, licensiering samt dataskyddsfrågor (PuL och Dataskyddsförordningen).


Wiersholm
Rune Opdahl
Henrik Aakrann

Endringer i Kommunikasjonsverndirektivet

I april 2016 annonserte EU-kommisjonen at den planla å revidere det såkalte Kommunikasjonsverndirektivet (direktiv 2002/58/EF). Det ble åpnet for høringsinnspill fra et bredt publikum.

Direktivets formål er å beskytte personvernet ved elektronisk kommunikasjon og kan sies å være en detaljering av retten til beskyttelse av kommunikasjon i artikkel 7 i EUs charter om grunnleggende rettigheter. Direktivet er fra 2002. I lys av den teknologiske utviklingen, og med tanke på å sikre overensstemmelse med EUs personvernforordning (forordning (EU) 2016/679), er en revisjon kjærkommen.

Høringsrunden viste stor interesse for forslaget. Det kom inn hele 421 høringssvar, herunder fra Artikkel 29-gruppen, som blant annet tar til orde for følgende:

1. Direktivets virkeområde må utvides til også å gjelde nye typer kommunikasjon, slik som meldingstjenester i sosiale medier og IP-telefoni.

2. Det klare utgangspunktet bør være at samtykke må innhentes, også for behandling av metadata som trafikkdata og lokasjonsdata. Det bør legges til grunn samme samtykkekrav som i EUs personvernforordning. Dette vil innebære at brukerne må gis en reell mulighet til å avstå fra å samtykke, slik at samtykke ikke kan være en betingelse for å bruke en tjeneste.

3. Bestemmelsen om bruk av informasjonskapsler bør omformuleres til å omfatte andre former for liknende teknologi som brukes til samme formål.

De øvrige høringssvarene viser, ikke overraskende, et klart sprik mellom synspunktene til næringslivet og individer. Borgerne ønsker gjennomgående strengere og mer spesifikk regulering. Eksempelvis ga 77 % av borgere og 70 % av statlige organer uttrykk for at tjenesteleverandører bør ha en plikt til å levere tjenester selv om brukere motsetter seg lagring av identifikatorer, slik som informasjonskapsler. Kun ¼ av bedriftene mente det samme.

Høringssvarene viser spenninger om grunnleggende forhold i dagens digitale økonomi, der innsamling og bruk av personopplysninger danner grunnlaget for finansieringen av en rekke tjenester. Det blir spennende å se hvordan Kommisjonen vil balansere næringslivets interesser mot borgernes synspunkt i sitt forslag til revisjon av Kommunikasjonsverndirektivet. Vi vil følge utviklingen og komme med en oppdatering i *Lov&Data* når forslaget foreligger.

Rune Opdahl er partner og advokat i Advokatfirmaet Wiersholm, Oslo.

Henrik Aakrann er advokatfullmektig i Advokatfirmaet Wiersholm, Oslo.

BØKER

Nis Peter Dall, Jesper Langemark og Amalie Langebæk

Persondataforordningen: en håndbog for praktikere
København : Ex Tuto forlag, 2016
400 sider (inklusiv forordningsteksten på ca. 150 sider)
ISBN 978-87-92598-42-4

Den 25. maj 2016 trådte persondataforordningen (forordning (EU) 2016/679) i kraft med virkning fra den 25. maj 2018. Dette er en begivenhed som nok ikke er forbigået nogen af *Lov&Datas* læseres opmærksomhed, og omtalen af forordningen både under det langvarige forhandlingsforløb og efter vedtagelsen har været massiv. Vi kan også forvente en omfattende litteratur om forordningen i de kommende år. Med *»Persondataforordningen – en håndbog for praktikere«* foreligger den første danske bog om forordningen kun ca. tre måneder efter dens ikrafttræden (efterfølgende er også udkommet *»Den nye persondataret – persondataforordningen«* af Peter Blume, der anmeldes i et senere nummer af *Lov&Data*).

Bogen er opdelt i en »almindelig« og en »speciel« del. Den almindelige del består af 14 kapitler og omhandler de »klassiske« persondataretlige emneområder som f.eks. de grundlæggende behandlingsregler og principper, den registreredes rettigheder, sikkerhed og sanktioner men også nye emner under forordningen som data protection officer-funktionen og brug af adfærdskodeks, certificering og databeskyttelsesmærkning. Generelt giver kapitlerne i den almindelige del en god oversigtsmæssig introduktion til de enkelte emner og forordningens regulering. Den specielle del behandler en række udvalgte emner: tredjelandsoverførsler, virksomhedsoverdragelser, markedsføring, ansættelsesforhold, outsourcing og it-drift, sociale medier og nye teknologier. Emnerne i bogens specielle del omfatter områder af stor praktisk betydning og er generelt velvalgte (det kunne overvejes, om ikke overførsler til tredjelande burde have været medtaget i bogens almindelige del, men det er en detalje), om end nogle af dem næppe giver anledning til særlige overvejelser i relation til forordningen, jf. også bemærkningerne om forholdet mellem gældende ret og forordningen straks nedenfor. Det gælder også for disse kapitler, at de generelt er velskrevne og giver et godt overblik over de enkelte emner. I alt består de to dele af ca. 250 sider, der bl.a. inkluderer forskellige tjeklister til de enkelte kapitler. Herudover er forordningen inklusive præambeltekst optrykt i bogen, så det samlede sidetal er ca. 400, forordningen er således altid ved hånden.

Forfattere af persondataretlige fremstillinger har i de næste år den udfordring, at der reelt består to regelsæt, man må forholde sig til; dels det gældende persondatadirektiv (direktiv 95/46/EF) med tilhørende nationale implementeringslove, dels den kommende persondataforordning, på sigt suppleret af de nationale særregler, som forordningen hjemler mulighed for. Dette forudsætter nogle fremstillingstekniske valg, herunder hvordan vægtningen mellem disse to regelsæt skal være. Bogen har, som titlen også angiver, sit primære fokus på de kommende regler i forordningen. Dette betyder dog ikke, at teksten er helt løsrevet fra gældende ret. En række kapitler indledes således med en kort beskrivelse af de gældende regler i persondataloven. Andre kapitler har ikke en sådan indledende beskrivelse af gældende ret men angiver eksempelvis nogle steder i teksten, at det pågældende krav gælder både efter forordningen og persondataloven. Der er således ikke en ensartet inddragelse af gældende ret gennem bogen, ligesom der ikke er en mere systematisk beskrivelse af forskellene på gældende ret og forordningen. Mens kapitlerne i den almindelige del konsekvent har sit primære fokus på forordningen, er nogle af kapitlerne og afsnittene i den specielle del primært en beskrivelse af gældende ret med ingen eller kun en ganske begrænset beskrivelse af forordningen. I disse kapitler følger bogen således ikke konsekvent sit eget formål om at introducere forordningen og det havde fremstået mere stringent, hvis afvejningen mellem beskrivelserne af gældende ret og forordningen havde været mere entydig gennem bogen. Forskellen på gældende ret og de kommende regler havde også stået tydeligere for læseren, hvis kapitlerne i den specielle del havde koncentreret sig om de temaer, hvor sådanne forskelle består.

Trods disse bemærkninger, er der samlet set tale om en velskrevet introduktion til forordningen, der på en komprimeret måde kommer omkring de relevante emner, hvilket i sig selv er en bedrift henset til hvor omfattende emneområder, der skal dækkes. Det er åbenbart, at en samlet beskrivelse af forordningen på ca. 250 sider nødvendigvis må få en oversigtsmæssig karakter. Som forfatterne selv anfører, er der ikke tale om en akademisk fremstilling, og bogen søger da heller ikke at give svar på de mange og vanskelige fortolkningsspørgsmål, som forordningen rejser eller at foretage nærmere analyser af det i praksis meget vigtige spørgsmål om forskellen mellem gældende ret og forordningens regler. Dens formål er at give en oversigtsmæssig introduktion til forordningen, og dette formål opfylder bogen overordnet set fint. Den kan derfor også anbefales til dem, der ønsker en sådan introduktion.

(Bogomtale ved Henrik Udsen, professor, dr.jur. ved Center for informations- og innovationsret (CIIR), Det Juridiske Fakultet, Københavns Universitet, og er en af de danske redaktører for Lov&Data.)


simonsen vogtwiig
Hedda Baumann Heier
Rune Ljostad

Høyesterett: Vurderingen av bransjelikhet etter foretaksnavneloven

Den 22. september 2016 kom Høyesterett med dom i HR-2016-1993-A. Saken gjaldt gyldigheten av et vedtak i Klagenemnda for industrielle rettigheter der registreringen av foretaksnavnet Pangea Property Partners AS ble ansett for å være i strid med foretaksnavneloven § 2-6 nr. 4. Spørsmålet i saken var om «Pangea Property Partners» var egnet til å forveksles med «Pangea».

Høyesterett presiserte at ved vurderingen av forvekslingsfare er kravene om kjennetegns- og bransjelikhet, som fremgår av foretaksnavneloven § 3-3 jf. § 3-2, å anse som kumulative krav (avsnitt 5). Det var i saken enighet om at det var stor kjennetegnslikhet mellom foretaksnavene. Tvisten knyttet seg til vurderingen av bransjelikhet. Vurderingstema for drøftelsen av bransjelikhet er om foretaksnavnet brukes for virksomhet av samme eller «*liknende slag*», jf. foretaksnavneloven § 3-3 (1).

Etter en gjennomgang av rettskildene på området oppsummerer Høyesterett det slik at bransjelikhet vil kunne foreligge «*dersom tjenestene alternativt er av samme art, har felles formål, anvendelse, distribusjonskanaler eller omsetningskrets, eller supplerer eller står i konkurranseforhold til hverandre*» (avsnitt 61). Det er ikke ansett tilstrekkelig at selskapene opererer på samme virksomhetsområde, men må i stedet avgjøres på bakgrunn av hvilke typer tjenester foretakene faktisk tilbyr. Dette nødvendiggjør at virksomhetene blir sammenliknet på «*relevant abstraksjonsnivå*» (avsnitt 62). For øvrig ble minimumskravet om til hva som er virksomhet av liknende slag i lovens forstand, ikke ansett for å være særlig strengt (avsnitt 64).

Konkret i saken kom Høyesterett til at det at sammenlikningen må foretas på relevant abstraksjonsnivå, tilsa at likhet ikke kunne utledes av at begge foretakene tilbød finansielle tjenester, men at det i stedet måtte foretas en undersøkelse av hvilke tjenester foretakene faktisk tilbød (avsnitt 66). Mens Pangea AS' tjeneste gjaldt typisk forbrukerkreditt, gjaldt Pangea Property Partners tjeneste megling av salg og utvikling av store næringseiendommer. Førstnevnte tjeneste var hovedsakelig rettet mot forbrukere som er medlemmer av lag og foreninger, mens sistnevnte rettet seg derimot mot et begrenset og profesjonelt marked. Tjenestene ble heller ikke funnet å supplere hverandre eller være i konkurranse med hverandre.

Kravet til bransjelikhet ble etter en konkret vurdering ikke funnet å være oppfylt, og det forelå dermed ikke forvekslingsfare. Dommen er enstemmig.

Les dommen i Lovdatas database.

EU-domstolen: Ansvaret for opphavsrettskrenkelser begått av tredjemenn som benytter seg av et allment tilgjengelig Wi-Fi som stilles til disposisjon i forbindelse med markedsføring av egen virksomhet

Den 15. september 2016 ble det avsagt en dom av EU-domstolen i sak C-484/14. Saken gjaldt en person som drev en forretning som solgte lys- og lydsystemer. Forretningen tilbød gratis og åpent Wi-Fi for å lokke til seg potensielle kunder. I 2010 ble et musikkverk som Sony Music Entertainment Germany GmbH hadde opphavsretten til, ulovlig lastet ned av en kunde som benyttet seg av nettverkstilgangen. Det var således ikke butikkeieren selv som faktisk krenket opphavsretten til musikkverket. Spørsmålet for EU-domstolen var om butikkeieren likevel kunne holdes ansvarlig for opphavsrettskrenkelser begått av brukerne av nettverket som han stilte til deres disposisjon.

EU-domstolen la til grunn at en som tilbyr gratis Wi-Fi til allmennheten yter en informasjonssamfunnstjeneste etter direktivet om elektronisk handel (direktiv 2000/31/EF) artikkel 12 (1). Domstolen la videre til grunn at vilkårene for ansvarsfrihet var oppfylt. Dette tilsa at den som driver en butikk og som tilbyr

Wi-Fi-nettverk gratis, ikke blir ansvarlig for brudd på opphavsretten begått av brukere av dette. Direktivet stenger imidlertid ikke for at rettighetshavere kan henvende seg til nasjonale myndigheter eller domstoler for å pålegge vedkommende forretningseier å stoppe eller forhindre opphavsrettskrenkelser. Dette kan oppnås ved at forretningseieren pålegges å passordbeskytte nettverket på en slik måte at brukere må avsløre sin identitet før de kan få et passord. Denne løsningen ville etter domstolens mening medføre en rimelig balanse mellom, på den ene siden, opphavsrettighetene til rettighetsinnehaveren og, på den andre siden, friheten til å drive forretningsvirksomhet og informasjonsfriheten til nettverksbrukene. Slik identifiseringsplikt (og autentiseringsplikt) er allerede vanlig for offentlige telefontjenester, jf. ekomloven § 2-4 annet ledd.

Les dommen på EU-domstolens websider (Curia) - eller i Eur-Lex-databasen hos EU¸ som også finnes hos Lovdata.

EU-kommisjonen: Forslag til nytt opphavsrettsregelverk

Den 14. september 2016 lanserte EU-kommisjonen en pakke med en ny meddelelse samt forslag til to direktiver og to forordninger som er ment å modernisere det gjeldende opphavsrettsregelverket og tilpasse det til dagens Digital Single Market. Det er forventet at det vil komme ytterligere initiativ hva angår sanksjoner og håndhevelse i løpet av de neste månedene.

Les dokumentene her:

- Communication - Promoting a fair, efficient and competitive European copyright-based economy in the Digital Single Market: *https://ec.europa.eu/digital-single-market/en/news/promoting-fair-efficient-and-competitive-european-copyright-based-economy-digital-single-market*

- Proposal for a Regulation laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions: *https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-laying-down-rules-exercise-copyright-and-related-rights-applicable-certain*

- Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market: *https://ec.europa.eu/digital-single-market/en/news/proposal-directive-european-parliament-and-council-copyright-digital-single-market*

- Proposed Regulation on the cross-border exchange between the Union and third countries of accessible format copies of certain works for persons who are blind, visually impaired or print disabled: *https://ec.europa.eu/digital-single-market/en/news/proposed-regulation-cross-border-exchange-between-union-and-third-countries-accessible-format*

- Proposal for a Directive on permitted uses of works and other subject-matter protected by copyright and related rights for the benefit of persons who are blind, visually impaired or print disabled: *https://ec.europa.eu/digital-single-market/en/news/proposal-directive-permitted-uses-works-and-other-subject-matter-protected-copyright-and*

Hedda Baumann Heier er advokatfullmektig i advokatfirmaet Simonsen Vogt Wiig, Oslo, og Rune Ljostad er partner i samme firma.

Bird & Bird

Jerker Edström
Anna Rzewuska

Säkerhetskopior av datorprogram får inte säljas vidare utan rättsinnehavarens tillstånd

Vidareförsäljning av en säkerhetskopia av ett lagligen förvärvat datorprogramexemplar, utan rättsinnehavarens tillstånd, utgör upphovsrättsintrång, även om det ursprungliga fysiska mediet för datorprogramexemplaret i fråga skadades eller borttappades. Detta har EU-domstolen (”EUD”) slagit fast i ett nyligen meddelat beslut i mål om förhandsavgörande C-166/15[1] (nedan benämnt ”Ranks-målet”).

Spridningsrätten och dess konsumtion

En av de ekonomiska ensamrättigheter som en upphovsman åtnjuter till sitt verk utgör spridningsrätten, dvs. rätten att kontrollera all slags spridning till allmänheten, genom försäljning eller på annat sätt, av originalet av verket eller kopior av detta. Spridningsrätten till ett exemplar av ett verk upphör, förklaras ”konsumerad”, när exemplaret har överlåtits inom EES-området av upphovsmannen eller med dennes samtycke, vilket medför att det överlåtna exemplaret fritt får spridas vidare. Konsumtion av spridningsrätten gäller enbart det överlåtna exemplaret av verket och inte verket i sig.[2] Upphovsmannens övriga ensamrätter i förhållande till verket, såsom rätten till mångfaldigande, påverkas således inte. Konsumtionsprincipen gäller vidare inte sådana ”icke-fysiska” överlåtelser av exemplar som är att anse som tjänster.[3]

För datorprogram gäller konsumtionsprincipen i artikel 4.2 i direktiv 2009/24/EG (”Datorprogramdirektivet”).[4] Det har länge varit omstritt om konsumtionsprincipen täcker onlineöverföringar av exemplar av datorprogram eller om dessa överföringar ska anses utgöra tillhandahållande av en tjänst. Det framgår nämligen inte av Datorprogramdirektivet vad som anses med ”alla former av spridning till allmänheten, inbegripet uthyrning, av datorprogrammets original eller kopia”, såsom spridningsrätten definieras i artikel 4.1 (c). Att spridningsrätten kan konsumeras, om vissa förutsättningar är uppfyllda, oavsett om överlåtelsen avser ett fysiskt eller icke-fysiskt exemplar av datorprogram har EUD numera klargjort i mål C-128/11 (*UsedSoft mot Oracle*, ”UsedSoft-målet”).[5]

Bakgrund till Ranks-målet

Det aktuella målet om förhandsavgörande har sitt ursprung i brottmål, inlett i Lettland, mot de tilltalade, som under tre års tid sålt via en digital marknadsplats uppskattningsvis 3 000 exemplar av begagnade datorprogram utgivna av Microsoft Corp. Den ekonomiska skadan som Microsoft Corp. åsamkats uppskattats till EUR 265 514.[6]

Den hänskjutande domstolen har vänt sig till EUD för att få klarhet i om ett begagnat datorprogramexemplar med tillhörande licens, förvärvat och lagrat på ett medium som inte utgör det ursprungliga mediet, i ett fall där det ursprungliga mediet skadats och den första förvärvaren har raderat sitt exemplar, kan säljas vidare med tillämpning av regeln om konsumtion av spridningsrätten och om detta är förenligt med artiklarna 4 (a), 4 (c), 5.1 och 5.2 i direktiv 91/250/EEG.[7]

Det bör noteras att direktiv 91/250/EEG numera är kodifierat genom Datorprogramdirektivet, men ordalydelsen av de i Ranksmålet analyserade artiklarna har inte

förändrats i Datorprogramdirektivet (härefter refereras enbart till de i Ranks-målet relevanta artiklarna i direktivet 91/250/EEG).[8]

EUD:s tolkning och tillämpning av konsumtionsprincipen i Ranks-målet

EUD har i Ranks-målet konstaterat genom att hänvisa till UsedSoft-målet att den som lagligen förvärvat ett begagnat datorprogramexemplar har, med stöd av konsumtionsprincipen i artikel 4 (c), rätt att sälja vidare detta exemplar. Det har poängterats att konsumtionen av spridningsrätten endast gäller själva exemplaret av ett datorprogram och den tillhörande användarlicensen, och inte det fysiska mediet för det exemplaret.[9] Rättsinnehavaren får därmed inte förhindra vidareförsäljningen av ett begagnat exemplar, så länge överlåtelsen inte gör intrång i rättsinnehavarens ensamrätt till återgivning enligt artikel 4 (a). Detta innebär att åtgärder för återgivning av programmet måste antingen omfattas av rättsinnehavarens *tillstånd* eller falla under något av *undantagen* i artiklarna 5 och 6. Dessa undantag hänför sig bl.a. till åtgärder för dekompilering och framställning av nya exemplar av datorprogram, inbegripet säkerhetsexemplar, som är nödvändiga för att exemplarägaren ska kunna använda datorprogram i överensstämmelse med dess avsedda ändamål.

Säkerhetsexemplar får inte säljas i andra hand

EUD har påpekat att ett säkerhetsexemplar av ett datorprogram får framställas med stöd av artikel 5.2 förutsatt att exemplaret (i) framställs av den person som har rätt att använda programmet och (ii) är nödvändigt för den aktuella användningen av programmet. Eftersom artikel 5.2 innehåller ett undantag från rättsinnehavarens ensamrätt till återgivning har EUD erinrat om att den enligt EUD:s fasta rättspraxis ska tolkas restriktivt.[10]

I ljuset av detta utgör framställning av ett säkerhetsexemplar en ny återgivning av ett datorprogram, som enbart får ske för att tillgodose behoven hos den person som har rätt att använda programmet. Eftersom rättsinnehavarens spridningsrätt till ett säkerhetsexemplar inte har konsumerats får exemplaret sålunda inte överlåtas till tredje man utan rättsinnehavarens tillstånd. Detta gäller oavsett om det medium på vilket ett exemplar ursprungligen varit lagrat har skadats eller förlorats. Ett sådant förhållande rättfärdigar inte att ett nytt exemplar av datorprogrammet framställs och överlåts utan rättsinnehavarens tillstånd.[11]

Nödvändiga återgivningar av datorprogram – komplement till konsumtionsprincipen

EUD har dock poängterat att den som lagligen förvärvat en licens för obegränsad användning av ett datorprogram har rätt att ladda ned exemplar från rättsinnehavarens webbplats, t.ex. om det ursprungliga mediet skadats eller förlorats.[12] En sådan nedladdning är nödvändig för att programmet ska kunna användas ändamålsenligt och utgör därför en tillåten återgivning enligt undantagsregeln i artikel 5.1.[13] Vid tidpunkten för vidareförsäljningen av själva licensen till datorprogrammet måste dock samtliga nedladdade exemplar göras obrukbara för att inte göra intrång i rättsinnehavares ensamrätt till återgivning enligt artikel 4 (a).

Sammanfattande kommentarer

Det kommer alltid att finnas en viss efterfrågan för begagnade datorprogram, i synnerhet för äldre versioner som inte längre säljs på förstahandsmarknaden. Utgången i Ranks-målet utgör ett välkommet förtydligande av exemplarägarens rättigheter i ett vanligt förekommande fall vid handel med begagnade datorprogram, nämligen då denne inte längre kan använda det originalmedium som datorprogramexemplaret varit lagrat på. Det klargörs att även om exemplarägaren har rätt att framställa ett säkerhetsexemplar, förutsatt att detta är nödvändigt för dennes användning av programmet, får exemplarägaren inte sälja ett sådant säkerhetsexemplar i andra hand utan rättsinnehavarens tillstånd. Om exemplarägaren däremot innehar en licens för obegränsad användning av datorprogrammet kommer den nya förvärvaren av licensen ha rätt att ladda hem ett nytt exemplar från rättsinnehavarens webbplats, eftersom en nedladdning i ett dylikt fall är nödvändig för en ändamålsenlig användning av programmet.[14]

Jerker Edström är advokat och partner på advokatfirman Bird & Bird, Stockholm.

Anna Rzewuska är biträdande jurist på advokatfirman Bird & Bird ,Stockholm.

Noter

1 Mål C-166/15, *Aleksandrs Ranks och Jurijs Vasiļevičs* mot *Finanšu un ekonomisko noziegumu izmeklēšanas prokoratūra och Microsoft Corp.*

2 Konsumtionsprincipen avseende upphovsrättsliga verk förutom datorprogram återfinns i artikel 4.2 i direktiv 2001/29/EG (”Infosoc-direktivet”).

3 Se skäl nr 29 i Infosoc-direktivet: ”Frågan om konsumtion uppstår inte då det gäller tjänster, särskilt inte i fråga om online-tjänster.” Jfr i mål C-128/11 (*UsedSoft mot Oracle*).

4 Konsumtionsprincipen avseende datorprogram i artikel 4.2

i Datorprogramdirektivet utgör *lex specialis* i förhållande till konsumtionsprincipen i artikel 4.2 i Infosoc-direktivet (se not. 2 ovan och mål C-128/11).

5 EUD har förklarat att konsumtionen av spridningsrätten inträder efter den första försäljningen av ett exemplar av ett datorprogram som genomförs inom EES av rättsinnehavaren själv eller med dennes samtycke, oavsett om försäljningen avser ett fysiskt eller icke-fysiskt exemplar av programmet.

6 Skadan har beräknats utifrån de belopp som krediterats de tilltalades PayPal-konton.

7 Då de tilltalade står åtalade för gärningar som begicks mellan åren 2001-2004 är direktiv 91/250/EEG och inte Datorprogramdirektivet tillämpligt.

8 De i Ranks-målet aktuella bestämmelserna 4 (a), 4 (c), 5.1 och 5.2 i direktivet 91/250/EEG motsvarar de numera gällande artiklarna 4.1 (a), 4.1 (c), 4.2, 5.1 och 5.2 i Datorprogramdirektivet.

9 EUD har i UsedSoft-målet påpekat att försäljning av en licens för obegränsad användning av ett datorprogram är att likställa med en äganderättsövergång av ett exemplar av datorprogrammet.

10 EUD har hänvisat till avgörandet i mål C-145/10 (*Painer mot Standard VerlagsGmbH et al.*).

11 Det faktum att en bok har skadats innebär inte att ägaren till boken utan rättsinnehavarens tillstånd får kopiera boken och sälja kopian av boken i andra hand. Spridningsrätten till kopian har inte konsumerats. Se Generaladvokatens förslag till avgörande i Ranks-målet, pkt. 44. Se även mål C-419/13 (*Art & Allposters International BV mot Stichting Pictoright*).

12 EUD har i UsedSoft-målet konstaterat att ”nedladdningen av en kopia av ett datorprogram och ingåendet av ett licensavtal avseende användningen av denna kopia bildar en odelbar enhet. Nedladdningen av en kopia av datorprogrammet är nämligen meningslös om denna kopia inte kan användas av innehavaren.”

13 Utan undantagsregeln i artikel 5.1 skulle en förvärvare fortfarande behöva rättsinnehavarens tillstånd vid varje nedladdning av det förvärvade programmet. Enligt artikel 4.2 i Datorprogramdirektivet är det endast spridningsrätten som konsumeras.

14 EUD påpekar att det ankommer på den som förvärvar en licens för obegränsad användning av ett datorprogram att vid nedladdning av ett exemplar från rättsinnehavarens webbplats styrka att denne har förvärvat licensen lovligen.

KONFERANSER

eForvaltningskonferansen arrangeres 13.-14.2.2017. Mer informasjon vil bli å finne på *http://www.jus.uio.no/ifp/om/organisasjon/seri/arrangementer/2017/eforvaltningskonferansen.html*

IRIS 2017 Internationales Rechtsinformatik Symposion arrangeres 23.-25.2.2017 ved Universität Salzburg, Østerrike. Mer informasjon kan finnes på *http://www.univie.ac.at/RI/IRIS17/*

Icegov, 10th International Conference on Theory and Practice of Electronic Governance organiseres 7.-9.3.2017 i New Dehli, India. Interesserte kan finne mer informasjon på *http://www.icegov.org/*

Konferansen **«Offentlig digitalisering»** arrangeres 22.-23.3.2017 i Aarhus i regi av Dansk IT. 'Offentlig digitalisering' er den største danske konferanse, der stiller skarpt på digitaliseringen af den offentlige sektor. Interesserte kan finne mer informasjon på *https://dit.dk/da/Arrangementer/Konferencer/Offentlig%20digitalisering*

Fordham IP Conference 2017 - Annual Intellectual Property Law and Policy Conference arrangeres 20.-21.4.2017 i New York. Mer informasjon kan finnes på *http://fordhamipconference.com/*

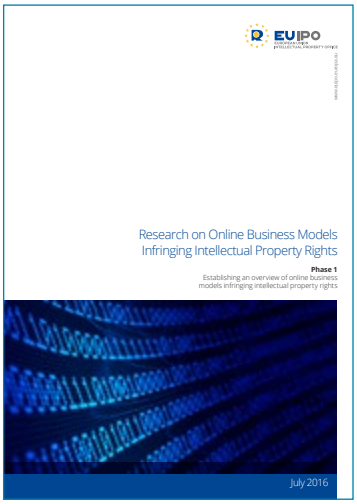
BILETA 2017 British and Irish Law Education and Technology Associations Annual Conference arrangeres 20.-21.4.2017 ved University of Hertfordshire School of Law. Mer informasjon kommer på *http://www.bileta.ac.uk/Annual%20Conference/*

2017 World Technology Law Conference arrangeres 3.-5.5.2017 i Chicago, USA.
Mer informasjon finnes på *https://www.eiseverywhere.com/ehome/chicago-2017/*

Gorrissen Federspiel

Janne Glæsel

EUIPO offentliggør rapport om online forretningsmodeller, der anvendes til at krænke immaterialrettigheder



The European Union Intellectual Property Office (EUIPO) udstedte i juli 2016 en rapport, der undersøger, hvilke online forretningsmodeller der krænker immaterialrettigheder. Formålet med undersøgelsen er at give et overblik over de forskellige krænkende forretningsmodeller, herunder hvordan de fungerer, er finansieret og giver overskud til deres bagmænd, samt hvilket indhold de udbreder og størrelsen på deres brugerbase. Det endegyldige mål er at identificere, analysere og udarbejde effektive strategier til bekæmpelsen af de krænkelser, der sker online.

Læs rapporten her:
https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/Research_on_Online_Business_Models_IBM/Research_on_Online_Business_Models_IBM_en.pdf

EUIPO har udarbejdet retningslinjer for behandlingen af ansøgninger om registrering af EF-designs

The European Union Intellectual Property Office (EUIPO) udstedte den 1. august 2016 retningslinjer for dennes behandling af ansøgninger om registrering af EF-designs. Formålet med retningslinjerne er at sikre ensartethed og sammenhæng i behandlingen af ansøgninger. Dette formål søges blandt andet opnået gennem generelle betingelser om: 1) begrundelse, 2) adressatens mulighed for at udtale sig om oplysninger, som afgørelsen er baseret på og 3) brugervenlighed.

Retningslinjerne gennemgår også kravene til ansøgninger om registrering af EF-designs, ansøgningsproceduren, behandlingen og vurderingen af ansøgningerne, betalingen af gebyrer, registreringen samt offentliggørelsen af EF-designet.

Læs retningslinjerne her:
https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/contentPdfs/law_and_practice/designs_practice_manual/WP_2_2016/examination_of_applications_for_registered_community_designs_en.pdf

EUIPO har udarbejdet retningslinjer for behandlingen af en ansøgning om fornyelse af registrerede EF-designs

The European Union Intellectual Property Office (EUIPO) udstedte den 1. august 2016 retningslinjer for behandling af ansøgninger om fornyelse af registrerede EF-designs.

Retningslinjerne angiver en række betingelser for ansøgninger, der skal opfyldes i forbindelse med fornyelse af EF-design, herunder: 1) ansøgerkredsen, 2) formkrav, 3) tidsfrister og 4) gebyrer. Derudover opstiller retningslinjerne visse krav til behandlingen af en ansøgning. Det fremgår blandt andet af retningslinjerne, at behandlingen er begrænset til en undersøgelse af, om de formelle betingelser er opfyldt. Der kan således ikke foretages en vurdering af, om designet er egnet til registrering. Når betingelserne er opfyldt, registreres fornyelsen. Fornyelsen træder i kraft dagen efter udløbet af den oprindelige registrering.

Læs retningslinjerne her:
https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/contentPdfs/law_and_practice/designs_practice_manual/WP_2_2016/registered_community_designs_renewal_en.pdf

Janne Glæsel er partner i advokatfirmaet Gorrissen Federspiel og er en av de danske redaktørene i Lov&Data.



SELMER

Martin B. Rove
Dan Sørensen
Ståle L Hagen

Er standardkontraktene tilpasset utnyttelse av «Big Data»?

«Big Data er informasjon som kjennetegnes ved høyt volum, høy hastighet og/eller høy grad av variasjon, og som krever nye metoder for prosessering og tilrettelegging for å kunne fungere som grunnlag for forbedrede beslutninger, økt innsikt og optimalisering av prosesser.» (Gartner, 2012 http://www.gartner.com)

IT-leverandører som leverer og drifter ulike systemer og løsninger (customer relationship management (CRM), enterprise resource planning (ERP) mv.), vil kunne ha stor nytte av å samle og analysere data om kundenes bruk av systemene de leverer, drifter og vedlikeholder. Ved å prosessere data fra mange kunder og sammenstille det med annen tilgjengelig informasjon, kan leverandørene få bedre grunnlag for å avdekke og rette opp i feil og mangler, utvikle stadig bedre løsninger samt tilby mer effektiv og treffsikker drift og support.

For å kunne gjøre det er leverandørene avhengige av å ha rettmessig og tilstrekkelig tilgang til og adgang til dataene. Men, er dagens standardavtaler tilpasset slik utnyttelse av data? Nedenfor trekkes frem noen eksempler fra Statens standardavtale for kjøp av driftstjenester (SSA-D).

SSA-D punkt 9.4 andre ledd første setning lyder:
«Leverandøren plikter å holde Kundens data logisk atskilt fra eventuelle tredjeparters data *for å eliminere faren for beskadigelse av data og/eller innsyn i data.»*

Punkt 10.3 lyder som følger:
«Kunden (og dennes rettighetsgivere) beholder eiendomsrett til alle data *som overlates til Leverandøren for behandling, og som lagres eller prosesseres ved hjelp av ytelsene under denne avtalen.* ***Det samme gjelder resultatet av Leverandørens behandling av slike data.***

Leverandøren har tilgang til data som nevnt ovenfor utelukkende i den utstrekning som er nødvendig for at Leverandøren skal kunne oppfylle sine forpliktelser i henhold til avtalen.»
(mine uthevinger)

Ved avslutning av avtaleforholdet fastlegger SSA-D blant annet følgende i punkt 4.4:
«Leverandøren har plikt til å legge til rette for at følgende blir overført til Kunden, eller til tredjepart utpekt av Kunden: "Kundens data inkludert de sikkerhetskopier av Kundens data som Kunden ønsker... Alle andre data og materiale som tilhører Kunden.»

Legger man ordlyden i SSA-D til grunn kan ikke ulike kunders data prosesseres sammen, kunden har eierskap til alle data som overlates til leverandøren (også som skapes ved kundens bruk?) og kunden har rett til resultatet av leverandørens behandling. I tillegg kan kunden kreve å få overført all data og alle kopier fra leverandøren ved opphør av avtalen.

Tatt på ordet, synes det utfordrende for driftsleverandørene å drive en noenlunde meningsfull Big Data-prosessering under en slik av-

tale. Det er nettopp prosessering fra ulike kilder (kunder) og eierskap til resultatene som gir grunnlag for de positive effektene nevnt ovenfor.

Dette bør leverandørene være oppmerksomme på, slik at de nødvendige endringer gjøres i avtalene for å gi får tilstrekkelige rettigheter til data. Kundene bør også være oppmerksomme på at ved å gi tilstrekkelige rettigheter (likevel med nødvendige begrensninger vedrørende konfidensialitet, personvern mv.), kan leverandøren settes i bedre stand til å levere bedre tjenester og produkter.

Kanskje bør det også vurderes endringer i standardavtalen eller et «Big Data-tillegg». Med dette er i det minste problemstillingen reist.

Martin B. Rove er advokat i avdelingen for Teknologi og Media i Advokatfirmaet Selmer DA, Oslo.

Ny standardavtale for leveranse av skytjenester

Den Norske Dataforening (DND) har tilgjengeliggjort en foreløpig versjon av en ny standardavtale for leveranse av skytjenester (skytjenesteavtale). Lansering av endelig versjon er ventet å skje i løpet av høsten 2016.

Skytjenester kjennetegnes ved av tjenestene leveres som ferdigpakkede standardisert tjenester. Skytjenester kategoriseres gjerne som programvare-, plattform- eller infrastrukturtjenester (SaaS, PaaS eller IaaS). Tjenestene kjennetegnes også ved at de normalt leveres globalt via internett og at kundens vederlag er knyttet til faktisk bruk eller utnyttelse av tjenestene.

Leverandørene av skytjenester krever som regel at deres egen standardavtale legges til grunn ved avtaleinngåelsen. Standardiseringene reduserer kundens mulighet til å få tilpasset leveransene til sine behov, men standardiseringene gir stordriftsfordeler som sikrer stabilitet, skalerbarhet og reduserte kostnader.

DNDs skytjenesteavtale legger opp til at partene skal gjennomføre et etableringsprosjekt med forberedelser, tilpasninger og testing, samt en godkjenningsperiode før leveransen går over i en eller flere ordinære tjenesteperioder. Avtalen regulerer også en særskilt avslutningsperiode ved opphør av avtaleforholdet. Disse reguleringene skiller seg ikke nevneverdig fra avtaler om leveranse av tradisjonelle driftstjenester.

Det ser imidlertid ut til at skytjenesteavtalen legger opp til at en eller flere standardiserte skytjenester leveres av en eller flere underleverandører, og at leverandøren under skytjenesteavtalen vil ta på seg rollen som en form for tjenesteintegrator av underleverandørenes skytjenester. En slik integratorrolle vil også kunne innebære utviklingsarbeid knyttet til integrasjoner og tilpasninger.

Det interessante spørsmålet blir hvilket ansvar leverandøren skal ha for underleverandørenes skytjenester. Det legges opp til at enkelte av underleverandørens avtalebetingelser kan inkluderes i skytjenesteavtalens bilag, men det er uklart hvordan denne utvelgelsen bør gjennomføres. Det er også usikkert hvilken aksept kundene vil gi for en slik mekanisme for videreføring av vilkår fra en eller flere underleverandører. Skytjenesteavtalen legger på den annen side til grunn at leverandøren blant annet skal levere i henhold til spesifikke krav til tjenestekvalitet (Service Level Agreement, SLA). Leverandøren skal også være ansvarlig for at skytjenestene er skalerbare, at data kan rekonstrueres ved behov og at kunden sikres rett til midlertidig å forlenge avtalen i forbindelse med avslutning av avtaleforholdet.

Det kan fort oppstå et klart motsetningsforhold mellom kundens krav til leveransene og hva leverandørens underleverandører faktisk forplikter seg til å levere. Dersom dette blir resultatet kan tjenesteintegratorens rolle endre seg fra leveranser og administrasjon, til risikohåndtering og «forsikring» mot gapet mellom kundens forventninger og det aktørene i markedet leverer. Det blir derfor interessant å se om dette motsetningsforholdet blir nærmere avklart når endelig versjon av avtalen lanseres.

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

Ståle L. Hagen er partner og leder av avdelingen for Teknologi og Media i Advokatfirmaet Selmer, Oslo

LINDAHL

David Frydlinger

Ansvarsbegränsningar i biträdesavtal – relevanta eller irrelevanta under General Data Protection Regulation (GDPR)?

Av nyheterna i EU:s Dataskyddsförordning (förordning (EU) 2016/679) som börjar tillämpas den 25 maj 2018, är det några som framträder mer än andra på grund av de långtgående konsekvenser de kommer att få. Två av dessa nyheter är de *radikalt ökade sanktionsnivåerna* vid överträdelser samt det faktum att *personuppgiftsbiträden genom förordningen kommer att få skyldigheter direkt enligt lag*.

Den senare nyheten väcker frågan om fördelning av ansvar för uppfyllande av förordningens skyldigheter mellan den personuppgiftsansvarige och personuppgiftsbiträdet. De ökade sanktionsnivåerna väcker vidare den i hög grad praktiska frågan om och i vilken mån en personuppgiftsansvarig och ett personuppgiftsbiträde genom avtal kan göra en ansvars- och riskfördelning som avviker från vad som anges i förordningen. Är det t.ex. möjligt för parterna att i personuppgiftsbiträdesavtalet införa en ansvarsbegränsning enligt vilken ett personuppgiftsbiträde bara ansvarar upp till ett visst maxbelopp för eventuella sanktionsavgifter eller skadestånd som den personuppgiftsansvarige åläggs att betala på grund av biträdets agerande i strid med förordningen eller biträdesavtalet? I denna artikel ämnar jag försöka kasta ljus på denna fråga, så gott det är möjligt i avsaknad av den rättspraxis på området som kommer att behöva utvecklas.

Utifrån personlig erfarenhet kan jag konstatera att många jurister inte verkar uppfatta att förordningen kommer att medföra någon skillnad från dagens läge när det gäller ansvarsbegränsningar i biträdesavtal. Det är idag inte ovanligt att biträdesavtal antingen inte innehåller ansvarsbegränsningar alls eller att det i huvudavtalet som hänvisar till biträdesavtalet anges att eventuella ansvarsbegränsningar inte gäller överträdelser av biträdesavtalet. Med andra ord är personuppgiftsbiträdets ansvar inte sällan obegränsat. Detta uppfattar många personuppgiftsbiträden som en ingalunda självklar ordning efter förordningens ikraftträdande, eftersom man upplever att risken med att acceptera obegränsat ansvar radikalt ökar. Och de personuppgiftsansvariga, som även de upplever en ökad risknivå, anser att de självklart borde i den mån det är möjligt, överföra delar av dessa risker till personuppgiftsbiträdet.

Men även om detaljerna i den nya ordningen inte är klara så är det utan tvekan så att förordningens ikraftträdande kommer att innebära förändringar från dagens läge när det gäller ansvarsbegränsningar. För att spetsa till det kan det faktiskt ifrågasättas om ansvarsbegränsningar i biträdesavtal över huvud taget kommer att ha fortsatt relevans.

Den personuppgiftsansvarige är enligt förordningen den som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Personuppgiftsbiträdet är den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Den vanligaste relationen mellan en ansvarig och ett biträde är relationen mellan en kund och en leverantör, exempelvis av IT-tjänster eller andra tjänster.

Liksom är fallet enligt dataskyddsdirektivet och 30 § personuppgiftslagen idag så måste en sådan relation regleras genom ett skriftligt avtal, vilket framgår av artikel 28 i förordningen. Artikeln utgör till stor del en kodifiering av dagens praxis avseende vad ett personuppgiftsbiträdesavtal ska innehålla, exempelvis att biträdet endast får behandla personuppgifter enligt den ansvariges skriftliga instruktioner och således inte för några egna ändamål. Avtalet måste även ålägga biträdet att vidta alla åtgärder avseende informationssäkerhet som anges i artikel 32. Biträdet måste också åläggas att bistå den ansvarige med att se till att skyldigheterna enligt artiklarna 32–36 fullgörs, t.ex. avseende informationssäkerhet, anmälan av personuppgiftsincidenter och konsekvensbedömningar.

Hänvisningarna till artikel 32 är här av särskilt intresse. Enligt denna

artikel åligger det nämligen *både den ansvarige och biträdet* att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en tillräcklig säkerhetsnivå med beaktande av de föreliggande riskerna. Detta är ett exempel på när förordningen ålägger biträdet självständiga skyldigheter.

Vad händer då om ett personuppgiftsbiträde endast vidtar undermåliga säkerhetsåtgärder och att detta får som konsekvens att en stor mängd av den ansvariges personuppgifter läcker ut, t.ex. genom att publiceras på internet? Det skulle t. ex., för att göra exemplet mer tillspetsat, kunna röra sig om personuppgifter om anställdas fackliga tillhörighet eller andra så kallade särskilda kategorier av personuppgifter. Antag att de anställda väcker skadeståndstalan om totalt 5 miljoner kronor mot sin arbetsgivare - den personuppgiftsansvarige - och att denne vill föra regresstalan mot biträdet. Antag dessutom att Datainspektionen inleder tillsyn och överväger att påföra sanktionsavgifter om ytterligare 5 miljoner kronor. Vilken betydelse skulle då en klausul i biträdesavtalet få som säger exempelvis att personuppgiftsbiträdet endast bär ett ansvar för brott mot biträdesavtalet uppgående till 1 miljon kronor? Skulle biträdet med framgång kunna åberopa denna klausul vid domstol?

Vad gäller *skadeståndsansvaret* framgår av artikel 82.1 i förordningen att varje person som har lidit materiell eller immateriell skada till följd av överträdelser av förordningen ska ha rätt till ersättning *från den personuppgiftsansvarige eller personuppgiftsbiträdet* för den uppkomna skadan. Av artikel 82.2 framgår att biträdet endast är ansvarigt om denne inte har fullgjort skyldigheter i förordningen som specifikt riktar sig till biträdet eller har agerat utanför eller i strid med den personuppgiftsansvariges lagenliga anvisningar. I det här exemplet, som rör bristande uppfyllande av säkerhetsåtgärder, skulle biträdet kunna bli ansvarigt både direkt för överträdelse av förordningens artikel 32 och för överträdelse av biträdesavtalet.

> För att spetsa till det kan det faktiskt ifrågasättas om ansvarsbegränsningar i biträdesavtal över huvud taget kommer att ha fortsatt relevans.

I artikel 82.4 anges att om t.ex. både en personuppgiftsansvarig och ett personuppgiftsbiträde har ”medverkat vid samma behandling” och dessutom är skadeståndsansvariga enligt artikel 82.1 så är de *solidariskt ansvariga* för skadan. En skadelidande kan därför vända sig till antingen den ansvarige eller biträdet och få full ersättning. I artikel 82.5 anges sedan att om någon av parterna har ålagts att erlägga full ersättning har denne rätt att föra regresstalan mot den andra parten till den del denne har orsakat skadan. Detta skulle tala för att en ansvarsbegränsning i biträdesavtalet inte skulle med framgång kunna åberopas av biträdet eftersom artikel 82.5 förstås är tvingande.

Artikel 82.5 är dock endast tillämplig om båda parter har ”medverkat vid samma behandling”. Det är oklart vad detta innebär exakt men jag antar dock här att en personuppgiftsansvarig som rätteligen har ålagt t.ex. en IT-leverantör att vida korrekta säkerhetsåtgärder inte kan anses ha ”medverkat vid samma behandling” om IT-leverantören sedan har brustit i att uppfylla denna skyldighet. Detta innebär att artikel 82.5, som endast är aktuell i situationer som avses i artikel 82.4, inte ens kommer att bli tillämplig i det här exemplet.

Om arbetsgivaren (den personuppgiftsansvarige) här ådöms skadeståndsansvar enligt artikel 82.1 men inte håller med domstolen om utfallet, kan denne förstås ändå föra regresstalan mot leverantören (personuppgiftsbiträdet). Artikel 82.5 är här, antar vi, inte tillämplig och en ansvarsbegränsning i biträdesavtalet skulle kanske kunna åberopas av biträdet. *Men först måste domstolen komma fram till att biträdet alls bär ansvar, trots att en domstol redan tidigare har kommit fram till att det är arbetsgivaren som är ansvarig.* Domen mot arbetsgivaren (den personuppgiftsansvarige) kommer förstås att få en kraftig bevisverkan i målet mellan den ansvarige och biträdet. Domstolen i det nya målet torde i de allra flesta fall göra samma bedömning som domstolen gjorde i det första målet och således komma fram till att det var arbetsgivaren (den personuppgiftsansvarige) som bar ansvaret. Frågan om ansvarsbegränsningen aktualiseras då aldrig.

I praktiken borde därför en ansvarsbegränsningsklausul aldrig bli relevant eftersom den ansvarige i första läget aldrig borde kunna åläggas skadeståndsansvar för en skada som har orsakats av biträdet. Gäller det samma - d.v.s. att ansvarsbegränsningen aldrig aktualiseras - avseende påförda *sanktionsavgifter*? Överträdelser av artikel 32 kan rendera sanktionsavgifter på upp till

2 % av den totala globala årsomsättningen för företag.

Naturligtvis gäller att endast den som har överträtt artikeln ska kunna åläggas sanktionsavgifter. I artikel 82.8 anges att tillsynsmyndighetens utövande av sina befogenheter att utdöma sanktionsavgifter ska omfattas av lämpliga rättssäkerhetsgarantier, vilka förstås bl.a. är till för att se till att inte fel part ådöms sanktionsavgifter. På samma sätt som i skadeståndsfallet kan sanktionsavgifter således endast påföras efter en bedömning av ansvarsfrågan, som kommer att inbegripa en bedömning av vem som har gjort och ansvarar för vad i samband med en överträdelse. Om Datainspektionen, i vårt exempel, skulle påföra den personuppgiftsansvarige sanktionsavgifter trots att denne har ställt rätt krav på personuppgiftsbiträdet, kommer den ansvarige sannolikt att överklaga detta beslut för att få ansvarsfrågan mellan den ansvarige och biträdet korrekt fastställd. När en lagakraftvunnen dom finns kommer ansvarsfrågan också att vara utredd.

Därför borde en ansvarsbegränsning i biträdesavtalet i praktiken inte heller bli relevant när det gäller frågan om sanktionsavgifter. Om, i vårt exempel, den arbetsgivaren (den personuppgiftsansvarige) väcker regresstalan mot IT-leverantören (personuppgiftsbiträdet) kommer domstolen sannolikt att avvisa talan som uppenbart ogrundad eftersom ansvarsfrågan när det gäller sanktionsavgifterna redan kommer att vara utredd.

> Därför borde en ansvarsbegränsning i biträdesavtalet i praktiken inte heller bli relevant när det gäller frågan om sanktionsavgifter.

Utifrån resonemanget ovan skulle en ansvarsbegränsning i biträdesavtalet således bli relevant endast i teorin vad gäller skadestånd och inte relevant alls det gäller sanktionsavgifter. Det återstår att se hur rättspraxis utvecklas.

David Frydlinger är advokat vid Advokatfirman Lindahl, Stockholm.

ANNET NYTT

Gorrissen Federspiel

Janne Glæsel

Forbrugerombudsmanden indskærper reglerne om markering af reklame

Den danske forbrugerombudsmand (Forbrugerombudsmanden) indskærpede den 19. juli 2016 reglerne om markering af reklame over for EF Sprogrejser, YouTube-netværket Splay og en kendt videoblogger (J. nr. 15/08873).

Sagen vedrørte en overtrædelse af lov nr. 1216 af 25. september 2013 (den danske markedsføringslov), hvori der stilles krav om, at reklamer skal være tydeligt markeret.

EF Sprogrejser havde indgået et samarbejde med en videoblogger om udarbejdelse af tre videoer. Kontakten var formidlet af Splay. Det fremgik ikke tydeligt af videoerne, at der var tale om reklame for sprogrejser. Forbrugerombudsmanden udtalte, at det skal være lysende klart for seeren, om en videobloggers indslag er for egen regning eller udgør en reklame, som bloggeren får penge for at deltage i. I den omhandlede sag var det vigtigt, at der ikke var tvivl om,

at der var tale om en reklame, og at der derfor ikke blot var tale om en glad pige, der på eget initiativ ville fortælle om sine gode oplevelser på en sprogrejse.

Forbrugerombudsmanden udtalte, at kravet i denne sag måtte skærpes, idet der var tale om produkter, der blev tilbudt til børn ned til tiårsalderen, og at videobloggeren selv var under 18 år. Forbrugerombudsmanden påbød videobloggeren at fjerne videoerne fra YouTube.

Læs udtalelsen her:
http://www.forbrugerombudsmanden.dk/Nyheder-fra-FO/Pressemeddelelser/2016/EF-Sprogrejser-og-Splay?tc=D74929A5CD4D4F43909476CBFC7C9FE1

Brugen af LinkedIn kontakters e-mailadresser til målrettet markedsføring på Facebook var lovlig

Den danske forbrugerombudsmand (Forbrugerombudsmanden) udtalte sig den 30. juni 2016 om, hvorvidt LinkedIn kontakters e-mailadresser lovligt kan kopieres og herefter anvendes på Facebook til at målrette annoncer i kontakternes nyhedsfeed. I sagen blev e-mailadresserne indtastet i Facebooks annoncesystem, hvorefter annoncerne blev vist i kontakternes nyhedsfeed. Ifølge Forbrugerombudsmanden er det uden samtykke generelt ulovligt for erhvervsdrivende at sende elektronisk post, hvis formålet er at afsætte varer eller tjenesteydelser.

Meddelelser i form af nyheder på Facebook anses som uønsket kommunikation, og modtagerne skal have adgang til at frabede sig disse meddelelser efter § 6, stk. 3 og stk. 5 i lov nr. 1216 af 25. september 2013 (den danske markedsføringslov). Ifølge Forbrugerombudsmanden er dette krav formentlig opfyldt, fordi meddelelserne på Facebook kan skjules af modtagerne ved at klikke i meddelelsernes højre hjørne. Forbrugerombudsmanden udtalte på denne baggrund, at det ikke er i strid med den danske markedsføringslovs § 6 at bruge LinkedIn kontakters e-mailadresser til målretning af annoncer i disse kontakters nyhedsfeed på Facebook.

Forbrugerombudsmanden understregede i sagen, at der ikke var foretaget en persondataretlig vurdering.

Læs udtalelsen her:
http://www.forbrugerombudsmanden.dk/Find-sager/Markedsfoeringsloven/Sager-efter-markedsfoeringsloven/spam0/Lovligt-at-maalrette-markedsfoering-paa-Facebook-ved-brug-af-LinkedIn-kontakters-emailadresser

Forbrugerombudsmanden udtaler, at artikler med omtaler og links, skal markeres, når der er tale om reklame

Den danske forbrugerombudsmand (Forbrugerombudsmanden) tog den 8. juli 2016 stilling til en sag, hvor et dagblads artikler omtalte og henviste til sin egen underside, der var sponsoreret, og i øvrigt linkede til andre selvstændige hjemmesider.

I sagen fremgik det kun af den sponsorerede underside, at der var tale om reklame. Artiklerne med henvisninger og links til denne underside var derimod ikke markeret som reklame. Ifølge Forbrugerombudsmandens var der i sagen tale om reklame, når artiklerne omtalte og henviste til undersiden. Det skulle derfor tydeligt markeres, at der var tale om reklame i toppen af omtalen. Da dette ikke var tilfældet, havde dagbladet overtrådt § 4 i lov nr. 1216 af 25. september 2013 (den danske markedsføringslov) og § 9, stk. 1 lov nr. 227 af 22. april 2002 (den danske e-handelslov).

I forbindelse med henvisningerne til de andre selvstændige hjemmesider fremgik det af sagen, at dagbladet ikke havde indgået aftaler om at omtale disse. Forbrugerombudsmanden udtalte, at hvis en sådan aftale er indgået, skal det tydeligt markeres i toppen af omtalen, at der foreligger en reklame. Ifølge Forbrugerombudsmanden gælder dette krav, uanset om der er truffet aftale om udformningen eller om indholdet i øvrigt indeholder redaktionelt stof. Desuden er det ikke afgørende for vurderingen af, om der er tale om en reklame, der skal markeres, at der modtages betaling for omtalen.

Læs udtalelsen her:
http://www.forbrugerombudsmanden.dk/Find-sager/Markedsfoeringsloven/Sager-efter-markedsfoeringsloven/skjultreklame/Artikler-med-omtaler-og-links-der-var-reklame-skulle-markeres

Janne Glæsel er partner i advokatfirmaet Gorrissen Federspiel og er en av de danske redaktørene i Lov&Data.

Returadresse:
Lovdata
Postboks 2016 Vika
NO-0125 Oslo
Norge

Nytt fra Lovdata

Avvikling av de trykte utgavene av Norsk Lovtidend

Justisdepartementet har besluttet å avvikle de trykte utgavene av Norsk Lovtidend avdeling I og avdeling II etter 2016-årgangen. Beslutningen er fattet etter råd fra Lovdata. Trykte registre for 2016-årgangen vil bli publisert i løpet av første kvartal 2017.

Antall abonnenter på den trykte utgaven har vært sterkt fallende over flere år. Den elektroniske kunngjøringen på *http://www.lovdata.no* har siden 2001 vært den offisielle kunngjøringen av Norsk Lovtidend.

Fra 1. januar 2017 blir det daglige kunngjøringer av Norsk Lovtidend avdeling I. For avdeling II vil kunngjøringsfrekvensen bli noe lavere. Kunngjøringene på *http://www.lovdata.no* vil i tillegg til den elektroniske kunngjøringen bli lagt ut på nettet som låste PDF-filer. Filene vil bli merket med dato og signert av Norsk Lovtidends redaktør. Det blir mulig å laste ned og å skrive ut dokumentene. Referanser til sidetall i heftene blir borte fra 2017-årgangen.

Lovdata kommer tilbake med nærmere informasjon om løsningen på våre nettsider.

Eventuelle spørsmål om avviklingen kan sendes på e-post til *lovtidend@lovdata.no* ev. kontakt Lovdata på *marked@lovdata.no* eller på telefon +47 23 11 83 00 for andre henvendelser.