JURIDISKA FAKULTETEN

vid Lunds universitet

Elisabeth Letzén

Ger svensk rätt ett tillräckligt skydd för personuppgifter vid anlitandet av molntjänster?

Examensarbete
30 högskolepoäng

Hans Henrik Lidgard

Immaterialrätt, Avtalsrätt

Termin 9

Innehåll

Summary

Cloud computing is a model for providing on-demand access to computing services via the Internet. The technology is not without a downside, which in this case is the privacy of personal information. This thesis provides an over-view of the Swedish legal position regarding the major issues of cloud computing privacy. In this respect, the thesis investigates how Personuppgiftslagen (1998:204) (PUL) and the Proposal for General Data Protection Regulation[1] handles the following matters; applicable law, duties and responsibilities of different players, the definition of consent, transfer of personal data to third countries, monitoring and sanctions.

Furthermore, the thesis contains a thorough examination of the different capabilities and functions of cloud computing from both an American and a European perspective. Firstly, by presenting the NIST Definition of Cloud Computing[2], which is an initiative from the U.S. Department of Commerce. This is by many seen as the most recognized definition. Secondly, by presenting the Article 29 data protection working group's act Opinion 05/2012[3].

Moreover, the thesis provides a detailed explanation of the legal position, including case reports made be the Swedish supervisory authority on Enköpings kommunstyrelse, Brevo AB and Salems kommunstyrelse, as well as a review of a report concerning cloud computing.[4]

The essay is completed with a section of analytical nature. In this respect, I have evaluated the problems that can occur in connection with protection of privacy when using cloud computing services. I have drawn my own conclusions concerning the legal situation and the risks the current law materializes along with the hazards the proposal possibly could bring forward.

The inference to be reached is that the Proposal for General Data Protection Regulation replaces a number of the deficiencies that can be seen in the current legislation. However, the issue is complex and many areas seem to

---

[1] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard of the processing of personal data and on the free movement of such data, European Commission, Brussels, 25.1.2012. COM(2012) 11 final.
[2] National Institute of Standards and Technology, *The NIST Definition of Cloud Computing*, Appendix A ("Bilaga A").
[3] Article 29 data protection working group, *Opinion 05/2012 on Cloud Computing*, Appendix A ("Bilaga B").
[4] The Swedish Supervisory authority's decisions in the cases: reference number: 256-2011, 574-2011, and 263-2011.

be unsolved or even aggravated by the proposal. The subject of privacy in “the cloud” is controversial and far from being uncomplicated.

Sammanfattning

Molntjänster möjliggör att en dator kan spara information i ”molnet” och att användare därmed kan tillgodogöra sig denna information under förutsättning att nätverksuppkoppling finns. Teknologin har dock vissa brister vad gäller skyddet av personuppgifter vid användning av molntjänster. Denna uppsats ger en överblick över rättsläget beträffande de största dilemman vilka uppkommer vid molntjänstanvändande vid behandling av personuppgifter. Härvid undersöks hur Personuppgiftslagen (1998:204) (PUL) samt förordningsförslaget; allmän dataskyddsförordning[5], hanterar frågor såsom gällande rätt, skyldigheter och ansvar för olika parter, definitionen av samtycke, överföring av personuppgifter till tredje land, tillsyn och sanktioner.

Uppsatsen innehåller vidare en beskrivning av molntjänsters egenskaper och funktioner från både ett amerikanskt och ett europeiskt perspektiv. För det första, beskrivs NIST Definition of Cloud Computing[6] vilken togs fram med initiativ från USA:s handelsdepartement. Denna definition är enligt många den mest etablerade och frekvent använda definitionen. För det andra, beskrivs Artikel 29-gruppens skrivelse; Opinion 05/2012[7].

Därefter redogörs i uppsatsen för det uppkomna rättsläget som innefattar datainspektionens föreskrift om molntjänster, beslut i tillsynsärendena Enköpings kommunstyrelse, Brevo AB samt Salems kommunstyrelse.[8]

Uppsatsen avslutas med en probleminventering och en konklusion med avslutande synpunkter. Härvid utreds de problem vilka kan uppkomma i relation till skydd av personuppgifter då molntjänster används. Jag har dragit mina egna slutsatser angående det rättsliga läget med den nuvarande lagstiftningen samt de konsekvenser förslaget skulle kunna ge upphov till. Den slutsats som nås är att förordningsförslaget ersätter ett antal av de brister vilka föreligger i dagens lagstiftning. Samtidigt konstateras att området är komplicerat och kontroversiellt vilket gör att flera frågor tycks förbli obesvarade.

---

[5] Översättning av: “Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard of the processing of personal data and on the free movement of such data”.

[6] National Institute of Standards and Technology, *The NIST Definition of Cloud Computing*, se Bilaga A.

[7] Article 29 data protection working group, *Opinion 05/2012 on Cloud Computing*, se Bilaga B.

[8] Datainspektionens beslut i ärendena: diarienummer: 256-2011, 574-2011, och 263-2011.

Förord

Jag vill rikta ett stort tack till:

Professor Hans Henrik Lidgard, min handledare, för engagemang, intresse och god vägledning,

Anna Hörnberg, jurist vid datainspektionen som har varit tålmodig med mina frågor,

David Törngren, rättssakkunnig vid Justitiedepartementet som svarat på mina frågor angående EU-kommissionens förslag om dataskyddsförordning,

Juridiska fakultetens IT support som har hjälp mig med diverse tekniska problem,

min familj som genom alla dessa år har stöttat mig igenom utbildningen,

Stockholm augusti 2012

Elisabeth Letzén

Förkortningar

Bet.	Betänkande
EES	Europeiska ekonomiska samarbetsområdet
EG	Europeiska gemenskapen
EU	Europeiska unionen
EU-kommissionen	Europeiska kommissionen
HD	Högsta domstolen
NJA	Nytt juridiskt arkiv
PUL	Personuppgiftslagen
Prop.	Regeringens proposition
SFS	Svensk författningssamling
SOU	Statens offentliga utredningar
SÖ	Sveriges överenskommelser med främmande makter

1. Inledning

Digitala fotavtryck skapas på Internet varje gång vi formar en digital personlig profil. Vi gör dessa profiler för att kunna få tillgång till nya tjänster, applikationer och lösningar för att förenkla och förbättra vår vardag. Samtidigt uppkommer risker och hot från detta digitala ymnighetshorn, i form av identitetsintrång och kränkning av den personliga integriteten. Personlig information, vare sig den är biologisk, genetisk, historisk, relationsrelaterad, yrkesrelaterad eller ryktesrelaterad, utgör vår nutida identitet. Därför är en uppdaterad lagstiftning vital för att ett effektivt skydd ska kunna föreligga. Närapå samtliga online aktiviteter, såsom skicka e-post, fylla i skattedeklarationen, hantera bankkonton, köpa varor och tjänster, koppla upp till ett företags intranät, möta människor i en virtuell värld, kräver överföring av identitetsinformation från en part till en annan. Idag behöver vi vanligtvis etablera en ny identitet varje gång vi använder en molntjänst[9]. Vi skapar denna identitet genom att fylla i ett online formulär och ge personlig information såsom namn, adress, kreditkortsnummer, telefonnummer osv. Internetanvändare efterlämnar personlig identifierbar information överallt utan att direkt ha kontroll över hur informationen används eller skyddas.

Rätten till skydd för personuppgifter föreligger i konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter och är skapad för att säkerställa att personuppgifter inte behandlas på ett potentiellt integritetskränkande sätt.[10] Artikel 5 i konventionen stadgar att alla uppgifter rörande en person inte är av sådan natur att de kan anses vara privata eller integritetskränkande. För att säkerställa att personuppgifter inte missbrukas garanterar rätten till skydd för personuppgifter att behandling av alla uppgifter om en person sker på ett öppet sätt som kan kontrolleras av den berörda individen.

Molntjänster som behandlar personuppgifter ökar i antal och blir allt mer betydelsefulla i samhället. Innebörden av denna nya teknologi är svår att överblicka. För att citera Nicholas G. Carr[11],

> "It will overturn strategic and operating assumptions, alter industrial economics, upset markets and pose daunting challenges to every user and vendor. The history of the commercial application of information technology has been characterized by astounding leaps, but nothing

[9] Innebörden av begreppet "molntjänst" förklaras under avsnitt 2.
[10] Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter.
[11] Nicholas George Carr är en amerikansk författare som har publicerat böcker och artiklar inom teknologi, ekonomi och kultur.

> that has come before – not even the introduction of the personal computer or the opening of the Internet – will match the upheaval that lies just over the horizon."[12]

Användandet av molntjänster växer och spelar en betydelsefull roll i många människors liv. Viljan att använda molntjänster kan emellertid hämmas av en oro för att uppgifterna inte skyddas på ett lämpligt sätt på grund av en icke anpassad lagstiftning. Lagstiftningen som tillämpas i Sverige idag vid behandling av personuppgifter är PUL och vid specialfall ett antal ytterligare regleringar.[13] PUL är en reglering som inträdde 1998 i syfte att implementera dataskyddsdirektivet 95/46/EG. Detta är nu nästan 14 år sedan och mycket har hänt sedan dess, inte minst vad gäller området för behandling av personuppgifter i molntjänster.

Den 25 januari 2012 offentliggjorde EU-kommissionen ett förslag om en allmän uppgiftsskyddsförordning, här kallad "allmän dataskyddsförordning" eller bara "dataskyddsförordningen".[14] Kommissionen framhöll i sin konsekvensanalys att nya utmaningar har uppkommit till följd av en snabb teknik- och affärsutveckling, vilket kräver en harmoniserad lagstiftning då en fragmenterad lagstiftning leder till osäkerhet kring säkerheten samt luckor vid tillämpligheten av lagen. Förslaget är i flera avseenden mer långtgående för skyddet av den personliga integriteten i jämförelse med den nuvarande lagstiftningen. Skulle förslaget gå igenom skulle det innebära en direkt tillämpning till följd av förordningsformen, utvidgad territoriell tillämpning, högre krav på samtycke och strängare sanktioner. Sverige med sin ovanligt omfattande grundlag vad gäller offentlighet och tryckfrihet har därför, inte helt överraskande, reagerat starkt på förslaget och regeringen har framfört i ett motiverat yttrande till EU-kommissionen att förslaget går för långt enligt subsidiaritetsprincipen. Ytterligare fyra medlemsstater[15] har invänt att EU får en alltför omfattande bestämmanderätt i och med förslaget.[16]

Behandling av personuppgifter inom molntjänster intresserar många då det inte sällan förenklar och effektiviserar arbete. Google införde nya

---

[12] Carr G., Nicholas, *The End of Corporate Computing,* MIT Sloan Management Review vol. 46, nr 3, 2005, s. 67-73.
[13] T.ex. myndighetsspecifika registerförfattningar och Offentlighets- och Sekretesslagen (2009:400).
[14] Riksdagen använder sig av namnet "allmän uppgiftsförordning" och justitiedepartementet använder sig av "allmän dataskyddsförordning", enligt uppgift från David Törngren vid Justitiedepartementet, 2012-04-27, kl. 10.00. De två namnen är översättningar av "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard of the processing of personal data and on the free movement of such data".
[15] Belgien, Frankrike, Italien och Tyskland.
[16] Interparliamentary Exchange, *Document COM/2012/0011*, http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20120011.do (2012-05-14, kl.14.00).

sekretessregler och användarvillkor den 1 mars 2012 i syfte att göra sina tjänster enklare och tydligare. Den franska dataskyddsmyndigheten, CNIL, har undersökt Googles användarvillkor och har ställt sig tveksamma om Google följer kraven i EU:s dataskyddsdirektiv. Under 2011 undersökte den svenska datainspektionen molntjänstanvändandet i samband med lagring av personuppgifter hos tre användare vilket resulterade i slutsatsen att brister förelåg i samtliga fall.[17]

Mot denna bakgrund ska denna uppsats utreda det nuvarande skyddet för personuppgifter i molntjänster och hur skyddet kan komma att ändras i och med det nya lagförslaget.

1.1 Syfte och problemformulering

Syftet med denna uppsats är att undersöka skyddet av personuppgifter vid anlitandet av molntjänster i dag samt vid en eventuell framtida lagförändring. Är de svenska reglerna tillräckliga eller behöver de modifieras? PUL, som grundar sig på ett EU-rättsligt direktiv är central vid skydd av personuppgifter. För att avgöra om dessa bestämmelser är tillräckliga måste först begreppet molntjänster undersökas samt PULs tillämpning vid skydd av molntjänster utredas. Mot bakgrund av det fastställda rättsläget kan sedan de svenska reglerna analyseras.

EU-kommissionens förslag om ny dataskyddsförordning, vilken är under förhandling för stunden behandlas också för att få en uppfattning om den framtida färdriktningen. Denna del av uppsatsen inriktar sig på att undersöka på vilket sätt förslaget skulle ändra dagens skydd och vilka effekter detta skulle komma att få på skyddet av personuppgifter och det fortsätta användandet av molntjänster. De frågor som behöver besvaras för att uppfylla uppsatsens syfte berör lagstiftningsform, territoriell tillämpning, överföring av personuppgifter till tredje land, krav på samtycke, molntjänsters användarvillkor, den personuppgiftsansvariges roll, missbruksregeln och hanteringsmodellen samt tillsyn vid överträdelse. Min ambition är att uppsatsen förhoppningsvis ska vara ett intressant inlägg i den rådande debatten om skydd av personuppgifter i molntjänster samt bidra till att ytterligare identifiera och analysera relevanta rättsfrågor.

[17] Datainspektionens beslut i ärendena: diarienummer: 256-2011, 574-2011, och 263-2011.

1.2 Metod och material

För att fastställa hur lagstiftningen ser ut vad gäller skydd för personuppgifter vilka behandlas i molntjänster har rättsdogmatisk metod används då syftet är att fastställa gällande rätt. I denna del av uppsatsen står svenska och EU-rättsliga lagstiftningsakter i fokus. För att få en fullständig bild av reglernas uppbyggnad och hur lagstiftaren anser att reglerna ska tillämpas har jag använt mig av svenska förarbeten. Praxis och doktrin har även använts som informationsskälla, dock i begränsad mån på grund av det knappa utbud som föreligger vad gäller gällande rätt vid behandling av personuppgifter i molntjänster inom Sverige och EU.

För att syftet med uppsatsen ska kunna uppnås har en förklaring av begreppet molntjänster varit nödvändig. Då det inte föreligger någon officiell definition har jag använt mig av två skrivelser jag har bedömt som relevanta. Dessa två förklaringar lägger grunden för innebörden av begreppet molntjänster vilken används i hela uppsatsen. Då molntjänster och dess omkringliggande egenskaper ofta benämns med engelska begrepp, föreligger en hel del engelska ord i uppsatsen i de fall jag har bedömt ingen passande svensk översättning föreligger.

Vad gäller studierna av rättspraxis har jag använt mig av tillsynsbeslut från datainspektionen då det är denna myndighet vilken kontrollerar om integritetsskyddet enligt PUL efterlevs. I skrivande stund föreligger tre beslut från datainspektionen angående molntjänstanvändning i samband med behandling av personuppgifter. I de fall PUL beskrivits i generella termer har beslut och domslut från andra instanser än datainspektionen använts för att ge läsaren en djupare insikt om lagens funktion.

Jag har vidare använt mig av en komparativ juridisk metod i syfte att utreda skillnader och likheter mellan PUL och EU-kommissionens förslag om dataskyddsförordning. Effekterna av dess skillnader har sedan analyserats ur ett juridiskt perspektiv. Tillvägagångssättet i denna del av uppsatsen har varit att på djupet gå igenom lagtext, förslag på lagtext, förarbeten, remissinstansers utlåtanden, Konstitutionsutskottets bedömning, regeringens bedömning om subsidiaritetsprincipen samt åsikter från sakkunniga. Utöver sakkunnigas åsikter som jag har hämtat ur artiklar samt doktrin, har jag även kontaktat ett antal personer över e-post och telefon. Jag förhåller mig inte till dessa sakkunnigas åsikter som en källa i egentlig bemärkelse, utan snarare som en inspiration till min egen analys. Det bör vidare understrykas att dataskyddsförordningen fortfarande är ett förslag under förhandling vilket gör att dess innehåll mycket väl kan komma att ändras. I denna uppsats beskrivs dock den version vilken EU-kommissionen offentliggjorde den 25 januari 2012, med vissa smärre modifikationer.

1.3 Avgränsning

Det vore alltför optimistiskt att göra en fullständig belysning och behandling av samtliga utländska rättssystem. Molntjänster verkar emellertid på en internationell nivå och har global tillgänglighet som måhända sitt mest tydliga kännetecken, vilket gör att analysen har gjorts i beaktande av viss internationell påverkan. Uppsatsen har dock främst haft svensk rätt, och därmed EU-rätt, som utgångspunkt.

Undersökningen av dataskyddsförordningen har avgränsats till de delar som påverkar skyddet av personuppgifter vid användandet av molntjänster. Förslaget har varit mycket omskrivet och genomgått en lång lagstiftningsförberedande process varför utrymme att behandla andra lagförslag eller alternativ till ändring av skyddet för personuppgifter inte ansetts föreligga. Samma sak gäller PUL, som har undersökts i de delar vilka är relevanta för att personuppgiftsskydd vid anlitandet av molntjänster. Mot denna bakgrund har jag gjort bedömningen att en fullständig analys och jämförelse av PUL och dataskyddsförordningen är en alltför stor uppgift. Analysen och utredningen fokuserar på skyddet av personuppgifter vid användandet av specifikt molntjänster. Andra problemställningar kopplade till dataskyddsförordningen och PUL faller utanför uppsatsen.

1.4 Disposition

Uppsatsen inleds i avsnitt 2 med en förklaring av molntjänsters egenskaper med hjälp av *NIST Definition of Cloud Computing* och Artikel 29-gruppens *Opinion 05/2012*. Avsnittet avslutas med en sammanfattning av molntjänsters generella funktioner uttolkat från de två skrivelserna.

Avsnitt 3 redogör för PULs grundläggande begrepp och regler vilka är relevanta vid skydd av personuppgifter. PUL beskrivs och utreds dels teoretiskt samt ur ett praktiskt perspektiv. Avsnittet avlutas med en sammanfattning av de begrepp och regler som beskrivits.

Avsnitt 4 behandlar rättsläget vid användande av molntjänster vid behandling av personuppgifter. Datainspektionens föreskrift om molntjänster redovisas samt de tre befintliga tillsynsärenden som gjorts vad gäller behandling av personuppgifter inom molntjänster. Avsnittet avslutas med en sammanfattning om det rådande rättsläget.

I avsnitt 5 presenteras EU-kommissionens förslag om allmän dataskyddsförordning i de delar som är relevanta vid behandling av personuppgifter i molntjänster. Eftersom de grundläggande begreppen vid personuppgiftsskydd redan redovisats i avsnitt 3 tas dessa inte upp igen. Avsnittet avslutas med en sammanfattning.

I avsnitt 6 analyseras de frågeställningar som formulerats i avsnitt 1.1. Frågeställningarna behandlas var för sig och utgör till stor del sammanställningar av de stegvisa konklusioner som gjorts genom uppsatsen. Uppsatsen avslutas sedan med en slutsats där jag kortfattat redogör för mina avslutande synpunkter.

2. Molnet och molntjänster

Internet har kommit in i en ny era tack vare mer tillförlitlig, kostnadseffektiv och tillgänglig uppkoppling, vilket gör att Internet inte bara är ett kommunikationsnätverk. Det har formats till att bli en plattform för en mängd olika typer av datoranvändande.[18] Flera termer har använts för att beskriva denna utvecklingsriktning för hur data hanteras och bearbetas. Istället för att använda mjukvara på en dator, är det numera möjligt att använda ”molnet”[19], ett nätverk av servrar, med syfte att kombinera mjukvara, data och datordrivkraft utspritt över Internet.[20] För att kunna konkretisera och åskådliggöra problematiken med skydd av personuppgifter inom molnet krävs en definition av begreppet. Det finns åtskilliga termer för tjänsterna i molnet vilket gör dem än mer komplexa.[21] Själva ordet ”molnet” kommer från den symbol som ofta används för att beteckna Internet när man gör ett diagram, ett moln, vilket i sin tur är taget från gamla ritningar där telefonverk ritades som moln.[22] Därefter har molnet blivit ett begrepp för platsen för så kallade molntjänster, vilket är en översättning av engelskans *cloud computing*.[23] I denna framställning kommer begreppet ”molntjänster” konsekvent användas för att undvika förvirring.

Det har förekommit en mängd försök för att få fram en enhetlig definition av molntjänster och forskare och experter försöker fortfarande enas om en korrekt klassifikation och terminologi.[24] Den mest etablerade definitionen, av molntjänster är NIST definition of Cloud Computing, vilken presenteras under avsnitt 2.1.[25] Artikel 29-gruppen[26], som är EU:s oberoende rådgivande instans för dataskydd och skydd av privatlivet, lade den 1 juli 2012 fram ett yttrande om en tolkning av innebörden av molntjänster och

---

[18] Hellström, Roger, *På molnfronten intet nytt? Vissa rättsliga aspekter på molntjänster*, Ny Juridik 2:11, 2011, s. 38.
[19] Översättning av: the cloud.
[20] Falk, Johan, *Cloud Computing Forskning & Framsteg*, nr 6/2009, s. 14.
[21] Svensson, Daniel, *Möjligheter och risker i Molnet*, Skydd & Säkerhet, Säkerhetsbranschens månadstidning, Nr 3:2011, s. 42-43.
[22] Molin, Åsa, *Att våga lita på webbmoln*, Dagen, s. 12-13.
[23] Christner, Anders & Edvardsson, Tobias. *Cloud Computing: en handledning och kommentar till IT & Telekomföretagens standardavtal Cloud Computing version 2010*, 2011, s. 11.
[24] Yousef, L., Butrico, M. & Da Silva, D., *Toward a Unified Ontology of Cloud Computing*, http://www.cs.ucsb.edu/~lyouseff/CCOntology/CloudOntology.pdf (2012-05-18, kl. 16.00).
[25] National Institute of Standards and Technology, *The NIST Definition of Cloud Computing*, se Bilaga A.
[26] Artikel 29-gruppen för skydd av personuppgifter, inrättades enligt artikel 29 i direktiv 95/46/EG. Gruppens arbetsuppgifter anges i artikel 30 i direktiv 95/46/EG och artikel 15 i direktiv 2002/58/EG.

dess risker.[27] Detta yttrande kommer kortfattat att presenteras under avsnitt 2.3.

2.1 NIST Definition of Cloud Computing

Den amerikanska federala organisationen för standarder och teknologi, NIST[28], har sedan november 2009 lagt fram 15 utkast till en definition av molntjänster. Den 16e och slutliga definitionen har publicerats som NIST Definition of Cloud Computing i syfte är att främja datasäkerhet.[29] Definitionen lyder enligt följande:

> "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[30]

Trots denna definition råder fortfarande oklarhet vad gäller begreppet. Nedan beskrivs fem karaktäristiska egenskaper som tillsammans, enligt NIST, är utmärkande för molntjänster.[31]

Egenskapen *on-demand self-service* innebär att användaren själv kan bestämma när tjänsten ska aktiveras och stängas av via ett administrativt system vilket gör att ingen eller begränsad kontakt krävs med varje enskild leverantör.[32] Denna egenskap kan hittas hos t.ex. digital-tv-boxar som erbjuder tv-kanaler *on demand*.[33]

En central egenskap är *broad network access v*ilket innebär att tjänsterna är disponibla genom ett öppet nätverk, dvs. Internet. Detta möjliggör att molntjänster är tillgängliga överallt via användande av exempelvis en smartphone, dator eller annan arbetsstation med nätverksuppkoppling.[34]

Den tredje egenskapen kallas *resource pooling* vilket innebär att resurserna i molnet delas med andra användare. Leverantörens datorresurser är

---

[27] Article 29 data protection working group, *Opinion 05/2012 on Cloud Computing*, se Bilaga B.
[28] Förkortning av: National Institute of Standards & Technology.
[29] *Final version of NIST Cloud Computing Definition Published*, NIST Tech Beat, 2011-10-25, http://www.nist.gov/itl/csd/cloud-102511.cfm (2012-03-29, kl.10.30).
[30] National Institute of Standards and Technology, a.a. s. 2.
[31] Ibid., s. 2.
[32] Ibid., s. 2.
[33] Copyswede, *SVT on demand i digital-tv-box*, http://www.copyswede.se/2012/01/svt-on-demand-i-digital-tv-box/ (2012-04-25, kl. 14.30).
[34] National Institute of Standards and Technology, a.a. s. 2.

sammansatta på ett sätt som ger service till ett stort antal konsumenter, vilka inte har någon direkt kontroll eller vetskap om var leverantörerna har sina datacenter geografiskt placerade. Egenskapen innebär att ett stort antal användare kan använda samma resurser samtidigt.[35] Citycloud[36], Google Drive[37], Dropbox[38], och iCloud[39] är alla exempel på molntjänster, som ger användare lagringsutrymme på leverantörens servrar. Tjänsterna kan förklaras som mappar på Internet vilka har samma funktioner som vanliga mappar på en dator med den enda skillnaden att leverantörerna automatiskt skickar upp innehållet, som sparas i mappen till en server, där innehållet kan läggas upp privat eller publikt.[40]

Molntjänster har vidare egenskapen att anpassas till användarens behov, antingen automatiskt eller efter användarens egna val, vilket kallas för *rapid elasticity*. Användare kan därmed använda molntjänster i den storlek och tidpunkt som passar dem bäst.[41]

Denna femte och sista egenskapen NIST använder för att beskriva molntjänster kallas *measured service* och innebär att molntjänster kan kontrollera, mäta och rapportera brukandet av tjänsterna. Detta kan ske genom exempelvis nyttjat lagringsutrymme, överförd datamängd eller antal aktiva konton. Transparensen kan erbjudas både för konsumenten och också för molntjänstleverantören.[42]

2.2 SPI-modellen

Vidare definierar NIST molntjänster genom att beskriva tre olika underkategorier, vilka inom IT-branschen tillsammans inte sällan benämns som SPI-modellen.[43] SPI-modellen är en förkortning av *Software as a Service* (Saas), *Platform as a Service* (PaaS) och *Infrastructure as a Service* (IaaS).

SaaS innebär att användaren nyttjar en programvara som tillhandahålls av en leverantör och kan ibland benämnas som *IT on demand* eller

---

[35] Ibid., s. 2.
[36] City Cloud – en molntjänst från City Network, http://www.citycloud.se/ (2012-04-04, kl. 16.00).
[37] Google Drive – en molntjänst från Google, https://drive.google.com/start (2012-04-25, kl. 16.00).
[38] Dropbox – en molntjänst, https://www.dropbox.com/ (2012-04-35, kl. 16.00).
[39] iCloud – en molntjänst från Apple, https://www.icloud.com/ (2012-04-25, kl. 16.00).
[40] Menken, Ivanka, *An introduction to Cloud Computing*, 2011, s. 150.
[41] National Institute of Standards and Technology, a.a. s. 2.
[42] Ibid., s. 2.
[43] Bl.a. Telia och Sungard använder SPI-modellen för att beskriva molntjänster på sina respektive hemsidor.

tillhandahållande av programvara enligt ASP-modellen[44]. Det innebär att användare kan få tillgång till mjukvara som tjänst över Internet.[45] Microsoft erbjuder exempelvis att användare kan prenumerera på Office, vilket möjliggör program för bland annat e-post, webbmöten, projektytor och ordbehandling, istället för att köpa programmet.[46]

PaaS innebär att molntjänstleverantören tillhandahåller en plattform där kunden kör sina egna datorprogram. I denna kategori kan användare skapa mjukvara med hjälp av verktyg och hjälpmedel från leverantören. Användaren kontrollerar mjukvarans spridning och uppbyggnad, samtidigt som leverantören tillhandahåller nätverket, servarna och lagringsutrymmet.[47] Ett exempel på denna typ av service är Google App Engine vilket är en tjänst som gör det möjligt för användare att skapa webbprogram som bygger på samma teknik som Googles webbplatser.[48]

Den tredje kategorin kallas IaaS och innebär att molntjänstleverantören tillhandahåller en infrastruktur som innehåller delar av nätverkskomponenter, lagringsutrymme, hårdvara, servrar osv. Leverantören äger dessa delar och är ansvarig för dess underhåll, funktion och reparation.[49] Användaren betalar oftast varje gång han eller hon använder infrastrukturen. City Cloud Service Provider Program är ett exempel på detta och är skapat för att möjliggöra för mjukvaru- och integrationsföretag att bredda utbudet av tjänster genom en server vilken ger mer datorkraft och diskutrymme.[50]

2.3 Artikel 29-gruppens yttrande om molntjänster

Enligt Artikel 29-gruppens yttrande Opinion 05/2012 består molntjänster av en mängd tekniska modeller vilka fokuserar bland annat på Internetbaserad användning och leverans av applikationer, processorkapacitet och lagring. Molntjänster ger möjlighet till virtuella system, vilka arbetar vid sidan om konventionella servrar under direkt kontroll av styrenheten, samt webbaserade programlösningar som ersätter konventionella program vilka

[44] Application Service Provider (ASP) innebär uthyrning av databaserade tjänster till användare över Internet.
[45] National Institute of Standards and Technology, a.a. s. 2.
[46] Microsoft Office, http://www.microsoft.com/sv-se/office365/online-software.aspx, (2012-05-16, kl. 13.00).
[47] National Institute of Standards and Technology, a.a. s. 3.
[48] Google App Engine, https://developers.google.com/appengine/ (2012-04-25, kl. 17.30).
[49] National Institute of Standards and Technology, a.a. s. 2-3.
[50] City Clouds affärsidé, http://www.citycloud.se/service-provider-2/ (2012-05-18, kl. 14.00).

är installerade på användarens dator. Dessa tjänster erbjuder sedan i praktiken bland annat ordbehandling, arkivsystem, lagring av dokument online, kalendersystem och e-post system.[51]

I bilagan till Opinion 05/2012 finns en kort sammanfattning av de egenskaper molntjänster erbjuder, vilka i stort liknar egenskaperna beskrivna i NIST Definition of Cloud Computing.[52] Mot denna bakgrund redovisas därför inte bilagan i Artikel 29-gruppens yttrande utan bifogas istället i Bilaga B.

2.4 Sammanfattning

NIST Definition of Cloud Computing och Artikel 29-gruppens Opinion 05/2012 kan båda sammanfattas på så sätt att molntjänster möjliggör att en dator kan spara information i ”molnet”, det vill säga på en annan server vilken går att komma åt via nätverksuppkoppling. Detta inkluderar information av typen e-post, ordbehandlingsdokument, kalkylprogram, filmer, patientjournaler, fotografier, finansiell information, affärsidéer, powerpoint presentationer, bokföringsinformation, marknadsföringskampanjer, försäljningssiffror, kalendermöten och mycket mer. Genom molntjänster är det även möjligt att använda program, nätverka via sociala medier och virtuella världar, kommunicera, överföra filer, se live-program och mycket mer.

[51] Article 29 data protection working group, a.a. s. 4.
[52] Ibid., s. 25-27.

3. Skyddet av personuppgifter i Sverige

Den grundläggande bestämmelsen om integritetsskydd vid automatiserad behandling av personuppgifter hittas i Regeringsformen (2011:109) 2 kap. 3 § 2 st. Där stadgas att varje medborgare, i den utsträckning som anges i lag, skall skyddas mot att hans eller hennes personliga integritet kränks genom att uppgifter om honom eller henne registreras med hjälp av automatisk databehandling. Sådana integritetsskyddande regler finns huvudsakligen i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och det fria flödet av sådana uppgifter (dataskyddsdirektivet). Syftet med direktivet är att skapa en gemensam nivå av integritetsskydd och därigenom möjliggöra ett fritt flöde av personuppgifter inom EU.[53] I Sverige skedde implementeringen av dataskyddsdirektivet den 24 oktober 1998 genom ikraftträdandet av PUL vilken ersatte den tidigare Datalagen (1973:289).[54] PULs syfte enligt PUL 1 § är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Syftet upprätthålls genom lagens bestämmelser om i vilka fall och under vilka förutsättningar personuppgifter får behandlas i samhället.[55] PUL är med andra ord i stort sett heltäckande vad gäller regleringen av skyddet för personuppgifter i Sverige. Mot denna bakgrund redogörs lagen nedan i de delar vilka anses relevanta för uppsatsens syfte.

PUL 3 § stadgar att den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter är *personuppgiftsansvarig*. Det innefattar normalt sett den juridiska person eller den myndighet som behandlar personuppgifter i sin verksamhet och som bestämmer vilka uppgifter som ska behandlas och vad de ska användas till.[56] Det kan vara svårt att bedöma vem som är personuppgiftsansvarig på förhand och det är en bedömning av fakta i varje enskilt fall. Avtal, lag, förordning eller särskilda registerlagar kan precisera vem som bär ansvaret, men det är de faktiska omständigheterna i det enskilda fallet som är avgörande.[57] *Personuppgiftsbiträde* är den som behandlar personuppgifter för den personuppgiftsansvariges räkning enligt PUL 3 §. Det kan t.ex. vara en molntjänst som anlitats av ett företag för att hantera företagets e-post.

---

[53] Ds 2001:27, s. 5.
[54] Prop. 1997/98:44, s. 1, bet. 1997/98:KU18.
[55] Öman, Sören & Lindblom, Hans-Olof, *Personuppgiftslagen, En kommentar*, 4e uppl., 2011, s. 11.
[56] Datainspektionen, *Personuppgiftsansvar*, 2010, s. 1 ff.
[57] Öman & Lindblom, a.a. s. 93.

Personuppgiftsbiträdet kan både vara en fysisk eller en juridisk person. Vid en felhantering av personuppgifter är det den personuppgiftsansvarige som kan få straff- eller skadeståndsansvar trots att denne anlitat ett biträde som utfört hanteringen.[58] Den *registrerade* är den som står i centrum när PUL tillämpas. Det är den registrerades personliga integritet som ska skyddas från en felaktig behandling av personuppgifter.[59]

3.1 Personuppgiftsbehandling som omfattas

PUL gäller för sådan behandling av personuppgifter som helt eller delvis är automatiserad enligt PUL 5 §. Behandling av personuppgifter innefattar enligt lagen varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatiskt väg eller inte, t.ex. genom insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring. Denna tolkning i PUL § 3 av begreppet ”behandling av personuppgifter” ger PUL ett vidsträckt tillämpningsområde.[60]

Känsliga personuppgifter är uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa och sexualliv enligt PUL § 13. Huvudregeln är att dessa uppgifter enbart får behandlas i fall då den registrerade angett sitt uttryckliga samtycke till behandlingen.[61] Ett flertal undantag föreligger dock för ett antal specifika fall vilka inte redovisas i denna uppsats.[62]

3.2 Definition av den registrerades samtycke

Samtycke definieras i lagen som varje slag av frivillig, särskild och otvetydig viljeyttring genom vilken den registrerade, efter att ha fått information, godtar behandling av personuppgifter som rör honom eller henne enligt PUL § 3. Artikel 29-gruppen har skrivit ett yttrande om definitionen av samtycke.[63] Av definitionen framgår att samtycket ska vara

---

[58] Blomberg, Kristina, *Värt att veta om Personuppgiftslagen*, 2012, s. 13.
[59] Ibid., s. 15.
[60] Öman & Lindblom, a.a. s. 119.
[61] Ibid., s. 282-288.
[62] Ibid., s. 288-291.
[63] Artikel 29-gruppen, *Yttrande 15/2011 om definitionen av begreppet ”samtycke”*,

en otvetydig viljeyttring vilket betyder att det inte bör finnas tvivel om att den registrerade avsett att frivilligt samtycka till behandlingen. Viljeyttringen ska vara uttrycklig på ett sätt så den är iakttagbar för en utomstående. Samtycket ska vidare vara frivilligt och informerat, dvs. lämnat efter det att information om behandlingen getts.[64] Det krävs inte att samtycket ska vara skriftligt, förutom i vissa specifika fall,[65] men vid tvist har den personuppgiftsansvarige bevisbördan för att samtycke har lämnats.[66] Samtycket ska vidare avse just den aktuella behandlingen av personuppgifter enligt datainspektionen. Samtycke till att ingå i viss undersökning innebär alltså inte automatiskt ett samtycke till den behandling av personuppgifter som genomförs inom ramen för undersökningen.[67]

NJA 2005 s. 361 klargjorde HD att ett samtycke till en viss behandling av personuppgifter måste finnas innan behandlingen påbörjas och kan inte med giltig verkan, åtminstone i straffrättsligt hänseende lämnas i efterhand.[68] Dock har datainspektionen ansett det vara tillåtet för tillhandahållaren av känsliga personuppgifter att inhämta samtycke i efterhand.[69]

Ett så kallat hypotetiskt samtycke är inte inkluderat i begreppet samtycke enligt definitionen. Oberoende av hur välgrundad hypotesen är om den registrerades inställning godtas det inte. Däremot kan ett tyst samtycke godtas i de fall det kan betraktas som en otvetydig viljeyttring då den registrerade informeras om en tilltänkt behandling och ges en frist för att motsätta sig för behandlingen.[70]

När den registrerade lägger in eller uppger uppgifter om sig själv, blir den registrerade automatiskt personuppgiftsansvarig och anses ha lämnat ett samtycke.[71] I de fall den registrerade inte kan avstå från att lämna ut sina personuppgifter kan inget samtycke anses föreligga. Då tveksamhet råder om frivillighet föreligger eller inte görs en bedömning utifrån villkoren i avtalet. I de fall varan eller tjänsten inte är nödvändig för den enskilde i dagens samhälle föreligger ett fritt val mellan att samtycka eller att avstå

01197/11/SV WP187.
[64] Ibid., s. 14.
[65] 9 § 2 st lagen (2002:546) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten (se prop. 2001/02:144, s. 33 f. och Ds 2001:67, s. 45 samt jämför prop. 2010:33 och prop. 2010/11:42 samt SFS 2011:127 angående borttagande av samtyckeskravet).
[66] Artikel 29-gruppen, a.a. 19.
[67] Datainspektionens rapport, 2002:4, s. 13, rapport 2003:1, s. 14.
[68] HDs dom den 26 maj 2005, NJA 2005, s. 361.
[69] Datainspektionens beslut 2008-08-06, diarienummer 217-2008.
[70] Artikel 29-gruppen, a.a. s. 19.
[71] Jmf prop. 2000/01:33, s. 114 f. och SOU 1999:105, s. 265 f.

från varan eller tjänsten.[72]

Vidare beaktas den registrerades beroendeställning till den personuppgiftsansvarige vid undersökningen om ett frivilligt samtycke föreligger eller inte.[73] I ett beslut av datainspektionen ansågs inte en registrerad person kunnat lämna ett frivilligt samtycke till företaget som behandlade uppgifterna då företaget vid tidpunkten hade monopol på tjänsten.[74]

PUL stadgar sex grunder när behandling av personuppgifter är tillåten utan den registrerades samtycke.[75] Dessa grunder lämnas dock utanför denna framställning då de inte anses viktiga för uppsatsens syfte.

3.3 PULs territoriella tillämpningsområde

PUL gäller för sådana personuppgiftsansvariga vilka är etablerade i Sverige enligt PUL 4 § 1 st. Svenska juridiska och fysiska personer och utländska filialer som bedriver verksamhet av mer permanent karaktär här i landet anses etablerade här.[76] Förarbetena tolkar denna bestämmelse så att då den personuppgiftsansvarige är etablerad i Sverige och utanför EU, skall den svenska lagen tillämpas på all verksamhet som den personuppgiftsansvarige bedriver inom detta område, men inte på den del som bedrivs utanför EU och EES. I de fall den enskilde är etablerad i ett land inom detta område, förutom Sverige, skall den svenska lagen enbart tillämpas på verksamheten i Sverige.[77] Punkt 19 i ingressen till EG-direktivet stadgar att en etablering är en ”effektiv och faktisk verksamhet med hjälp av en stabil struktur”.

Vidare tillämpas PUL även i fall då den personuppgiftsansvarige är etablerad i tredje land (ett land utanför EU eller EES) och använder sig av utrustning som finns i Sverige för behandlingen av personuppgifter. Detta betyder att ett amerikanskt företags insamling av personuppgifter här i landet omfattas av lagen, under förutsättning att företaget använder utrustning som finns här i Sverige. Lagen är dock inte tillämplig om utrustningen enbart används för att överföra uppgifter mellan ett tredje land och ett annat tredje land enligt PUL 4 § 2 st. Det som är problematiskt är att denna bestämmelse baseras på den oklara och svårtolkade artikel 4 i EG-direktivet. Eftersom artikeln berör frågor av internationell karaktär har det ansetts lämpligast att bestämmelsen i PUL enbart tar in de huvudregler som

[72] Artikel 29-gruppen, a.a. s. 20.
[73] Ibid., s. 13.
[74] Datainspektionens beslut 2007-10-08, diarienummer 246-2007.
[75] Öman & Lindblom, a.a. s. 225.
[76] Lindberg, Agne & Westman, Daniel, *Praktisk IT-rätt*, 3e uppl., 2001, s. 172.
[77] Ibid., s. 173.

otvetydigt framgår av artikeln.[78]

3.4 Överföring av personuppgifter till tredje land

Till följd av att lagstiftningen vad gäller skydd för personuppgifter skiljer sig avsevärt mellan länder, kan det variera stort i hur skyddet ser ut beroende på var uppgifterna befinner sig. Det föreligger ett förbud i PUL att överföra personuppgifter till tredje land som inte har en adekvat nivå för skydd av personuppgifter enligt PUL § 33. Bedömningen av om det föreligger en adekvat skyddsnivå i ett land eller inte bedöms med hänsyn till samtliga omständigheter som har samband med överföringen. Dessa omständigheter är bland annat uppgifternas art, ursprungslandet, ändamålet med behandlingen, tid för behandlingen, det slutliga bestämmelselandet och de regler som finns för behandlingen i det tredje landet.[79]

Tredje land är en stat som inte ingår i EU eller är anslutet till EES enligt PUL § 3. När PUL var ny ansågs publicering av personuppgifter på Internet jämställt med att föra över personuppgifter till tredje land.[80] Bodil-målet ändrade dock denna uppfattning till att Internetpublicering som sker från en server vilken ägs av någon som är etablerad inom EU och EES inte är att jämställa med överföring av personuppgifter till tredje land.[81] När någon sänder ett e-postmeddelande eller en fil som innehåller personuppgifter till någon annan i ett tredje land, föreligger en överföring till tredje land.[82]

Undantag från förbudet mot överföring till tredje land föreligger om den registrerade samtycker till överföringen. Mer om samtycke hittas under avsnitt 3.2. Även utan samtycke kan överföring av personuppgifter till tredje land vara tillåten. För det första är det tillåtet att utan samtycke från den registrerade att föra över uppgifter till tredje land om det är nödvändig för att ett avtal mellan den registrerade och den personuppgiftsansvarige ska kunna fullgöras. Detta kan vara exempelvis den överföring en resebyrå måste göra av resenärers personnummer för att kunna boka ett hotellrum i tredje land.[83] För det andra är det tillåtet utan den registrerades samtycke att föra över uppgifter till tredje land om det är nödvändigt för att ett avtal (vilket måste ligga i den registrerades intresse) mellan den personuppgiftsansvarige och tredje man ska kunna ingås eller fullgöras. Denna situation kan exempelvis uppkomma då personuppgifterna rör en

[78] Öman & Lindblom, a.a. s. 115.
[79] Ibid., s. 448.
[80] Blomberg, a.a. s. 97.
[81] Göta Hovrätts dom den 7 april 2004 i mål nr B-747/00.
[82] Blomberg, a.a. s. 97.
[83] Ibid., s. 98.

mottagare av en gåva, och företaget som levererar gåvan måste ha tillgång till uppgifterna för att sända gåvan. Den tredje situationen är då behandlingen är nödvändig för att vitala intressen för den registrerade ska kunna skyddas enligt PUL § 33.

Det är även tillåtet att föra över personuppgifter för användning i ett land som anslutit sig till dataskyddsdirektivet. EU-kommissionen har stadgat i Artikel 25.6 i dataskyddsdirektivet att följande stater innehar en adekvat skyddsnivå; Andorra, Argentina, Bailiwick of Guernsey, Färöarna, Isle of Man, Israel Jersey och Schweiz. Vidare har kommissionen bedömt att skyddsnivån är adekvat i Kanada om deras lagstiftning för skydd av personuppgifter i privat sektor är tillämplig på mottagarens personuppgiftsbehandling, samt i USA om mottagaren har anslutit sig till de så kallade Safe Harbor-principerna.[84] Dessa principer är en samling frivilliga regler, vilka organisationer i USA kan ansluta sig till, som rör personlig integritet och dataskydd och har tagits fram och beslutats av USA:s handelsdepartement[85].

3.4.1 EU-kommissionens standardklausuler

Det finns dock möjlighet att komma undan regeln om adekvat skyddsnivå genom att använda någon av de tre standardklausuler som godkänts av EU-kommissionen.[86] Dessa standardklausuler togs fram för att underlätta dataflöden från gemenskapen. I kommissionens beslut om framtagandet av klausulerna stadgas att bristen på globala dataskyddsbestämmelser gör standardklausuler till ett viktigt verktyg vid överföring av personuppgifter från alla medlemsstater.[87] Standardklausulerna är enbart en mall eftersom all dataöverföring är frivillig och därmed kan dataöverförare välja fritt bland de tre standardklausulerna eller välja annan rättslig grund för dataöverföring. Dock kan inte själva utformningen av mallarna ändras eller kombineras. Standardklausulerna syftar till att öka tillämpningen av avtalsklausuler genom mer flexibla redovisningskrav och mer detaljerade bestämmelser om rätten till tillgång.[88]

---

[84] Europeiska kommissionen, *beslut av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbor Privacy Principles) i kombination med frågor och svar som Förenta staterna handelsministerium utfärdat EGT L 215*, 2000-08-25, s. 7-47.
[85] Översättning av: Department of Commerce.
[86] Europeiska kommissionens standardklausuler, www.ec.europa.eu (2012-06-01, kl. 14.00).
[87] Europeiska kommissionen, *beslut av den 27 december 2004 om ändring av beslut 2001/497/EG om standardavtalsklausuler för överföring av personuppgifter till tredje land*.
[88] Ibid., s. 1-4.

3.4.2 Användarvillkor

Binding Corporate Rules eller användarvillkor är regler som en koncern med bolag i olika länder (inklusive länder som tillhör tredje land) själv kan ta fram för att reglera sin egen behandling av personuppgifter.[89] Överföring av personuppgifter till tredje land tillåts utan den registrerades samtycke, om det finns tillräckliga garantier i användarvillkoren för skydd av den registrerades rättigheter. Under våren har Google varit i blåsvädret efter att de införde ett nytt användarvillkor den 1 mars 2012 för sina samtliga tjänster.[90] De nya villkoren innebär i korthet att användaren enbart behöver godkänna ett avtal och att Google kan använda användarinformation mellan sina tjänster för att kartlägga användarens aktivitet. Denna kartläggning används sedan för att kunna göra tjänsterna skräddarsydda för användaren samtidigt som anpassad reklam riktas mot användaren.[91] Det följande står i det nya användaravtalet:

> ”När du lägger upp eller på annat sätt skickar in innehåll till våra tjänster ger du Google (och våra samarbetspartner) en global licens att använda, värdlagra, spara, återge, ändra, skapa härledda verk (exempelvis översättningar, anpassningar eller modifieringar som vi gör så att ditt innehåll fungerar bättre med våra tjänster), kommunicera, publicera, framföra offentligt och distribuera innehållet. Rättigheterna som du beviljar i licensen gäller endast i syfte att driva, marknadsföra och förbättra våra tjänster, samt utveckla nya tjänster. Denna licens fortsätter att gälla även om du upphör att använda våra tjänster (exempelvis företagsuppgifter som du har lagt till i Google Maps). I vissa tjänster är det möjligt att komma åt och ta bort innehåll som har skickats till tjänsten. I en del av våra tjänster finns det också villkor eller inställningar som begränsar vår användning av innehåll som skickas till tjänsterna.” [92]

De två sista raderna har ändrats under våren 2012 från att Google gav sig själv rätten att äga användarinformation i all framtid utan möjligheter till begränsning. Villkoren är dock fortfarande långtgående vilket har gjort att den franska dataskyddsmyndigheten, CNIL, har på de övriga europeiska dataskyddsmyndigheternas vägnar, ställt 69 frågor till Google.[93] Frågorna berör bland annat om Google använder sig av ansiktsigenkänning, hur annonser fungerar och hur GSP-platser behandlas och varför Google inte tar

---

[89] Blomberg, a.a. s. 102.
[90] Googles användarvillkor, http://www.google.com/policies/terms/ (2012-05-24, kl.15.30).
[91] Googles policyer och principer, http://www.google.com/intl/sv/policies/ (2012-05-19, kl. 14.00).
[92] Googles användarvillkor, a.a.
[93] *CNILs 69 frågor till Google*, http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/questionnaire_to_Google-2012-03-16.pdf (2012-06-19).

bort användarinformation från sina system när användare tar bort sitt konto. Google riskerar att få böta upp till 560 miljoner euro om företaget inte följer dataskyddsdirektivet enligt Europaportalen.[94] I en artikel i Dagens Nyheter intervjuades datainspektionens jurist Jonas Agnvall där han uttalade att det kan vara knepigt att få internationella företag att ändra sina användarvillkor.[95] Hur Google bemött CNILs frågor är i skrivande stund oklart. Jonas Agnvall säger i artikeln att i det fall CNIL och Google inte kommer överens, blir det upp till varje lands myndigheter att försöka få Google att följa sin lagstiftning, i Sveriges fall PUL. Agnvall berättar att det först kommer skötas på dialognivå men att det sedan finns möjlighet att böter eller andra sanktioner kommer användas. Avstängning av Googles tjänster i något land ser han som osannolikt.[96] Det är ännu är oklart om Googles användarvillkor strider mot dataskyddsdirektivet, då utgången av CNILs granskning ännu ligger i framtiden. Google är enbart en av många molntjänster som använder sig av personuppgifter och användarinformation i vinstsyfte. Hur denna strid avgörs kommer fastställa i mångt och mycket hur nuvarande lagstiftning står sig mot stora molntjänstleverantörer vilka verkar utanför EU och EES.[97]

3.5 Hanteringsreglerna och missbruksregeln

Den 1 januari 2007 ändrades PUL såtillvida att beroende på om personuppgifterna är strukturerade eller ostrukturerade avgörs vilka regler i lagen som gäller.[98] I de fall personuppgifter förekommer i ett register, exempelvis i en databas, anses uppgifterna vara strukturerade. Återfinns däremot uppgifterna i exempelvis e-postprogram anses uppgifterna vara ostrukturerade. Reglerna för strukturerade uppgifter kallas hanteringsreglerna och är betydligt strängare än missbruksregeln vilken gäller för ostrukturerad behandling.[99] Förändringen har lett till att den som hanterar personuppgifter i ostrukturerad form, till exempel löpande text på Internet, eller använder vanliga filsystem och e-postprogram, lägger ut

---

[94] Haglund, Fredrik, *Europeiska dataskyddsmyndigheter har bett Google svara på en rad frågor om företagets nya användarvillkor*, Europaportalen, http://www.europaportalen.se/2012/03/europeiska-datamyndigheter-ifragasatter-google (2012-05-24, kl.15.30).
[95] Rolfer, Andreas, *Knepigt få Google att ändra sig*, Dagens Nyheter, http://www.dn.se/ekonomi/knepigt-fa-google-att-andra-sig?rm=print (2012-05-24, kl.15.00).
[96] Ibid.
[97] Rejdnell, Jan, *Den personliga integriteten behöver stärkas*, Newsmill, http://www.newsmill.se/artikel/2012/03/29/nu-beh-vs-konkreta-f-rslag-att-st-rka-personliga-integriteten (2012-05-28, kl. 15.00).
[98] Prop. 2005/06:173, s. 1.
[99] Ibid., s. 18.

personbilder på Internet, konverserar i sociala medier som Facebook m.m. inte behöver vara belastad med krav på överväganden om tillåtligheten, fullgörandet av informationsskyldigheter osv.[100] Enligt missbruksregeln är behandlingen av personuppgifter tillåten så länge behandlingen inte kränker den personliga integriteten.[101]

Genom införandet av reglerna har nya gränsdragningsproblem skapats. Digitalt material är ofta strukturerat, sökbart och sammanställbart, vilket gör att det denna typ av behandling omfattas av hanteringsreglerna.[102] Enligt förarbetena ska regelrätta register och databaser omfattas av hanteringsreglerna, dock inte personuppgifter i löpande text, eller enstaka ljud- och bildupptagningar där det centrala är bilden eller ljudet. Tillämpningen av hanteringsreglerna kräver vidare att personuppgifterna omfattas av någon form av indexering som tar sin utgångspunkt i just personuppgifterna, dvs. att personuppgifterna utgör det centrala.[103] Detta innebär att medveten indexering omfattas av hanteringsreglerna, men inte sökningar på sökmotorer eller namnlistor på Internet.[104]

3.6 Tillsyn

Datainspektionen är den myndighet som utför tillsyn vid misstanke om överträdelser av PULs regler. Inspektionen kan enligt PUL § 45 vid vite förbjuda den personuppgiftsansvarige att fortsätta att behandla personuppgifterna om denne inte efter påpekanden eller liknande förfaranden gjort rättelser. Den personuppgiftsansvarige får i ett sådant fall, trots att han inte får fortsätta behandla uppgifterna, fortsätta lagra dem. Datainspektionen gör inspektioner på plats eller så kallade skrivbordsinspektioner vilket innebär att inspektionen skriver en varning till den personuppgiftsansvarige. Allmänheten kan även göra en anmälan till datainspektionen. I första hand eftersträvar datainspektionen att kommunicera med den personuppgiftsansvarige och i andra hand hamnar

---

[100] Grundläggande krav på behandlingen av personuppgifter (9 §), När behandling av personuppgifter är tillåten (10 §), Förbud mot behandling av känsliga personuppgifter (13 - 19 §§), Uppgifter om lagöverträdelser (21 §), Personnummer (22 §), Information till de registrerade (23–26 §§), Rättelse (28 §), Förbud mot överföring av personuppgifter till tredje land (33 och 34 §§), Upplysningar till allmänheten om behandlingar som inte har anmälts (42 §).

[101] Prop. 2005/06:173, s. 1.

[102] Björklund, Karl-Fredrik & Johnssén, Filip, *Nya förenklade regler i personuppgiftslagen*, Advokaten, nr 7, 2007, Årgång 73.
http://www.advokatsamfundet.se/Advokaten/Tidningsnummer/2007/Nr-7-2007-Argang-73/Nya-forenklade-regler-i-personuppgiftslagen/ (2012-06-19, kl. 15.00).

[103] Prop. 2005/06:173, s. 20-21.

[104] Björklund & Johnssén, a.a.

vite.[105]

Den personuppgiftsansvarige ska betala skadestånd om denne behandlat uppgifterna i strid med reglerna i PUL. Detta kan ske då den registrerade råkat ut för skada eller kränkning genom den felaktiga behandlingen. Det krävs inget uppsåt eller ens att den personuppgiftsansvarige varit oaktsam. Den registrerade behöver enbart visa att behandlingen stridit mot lagen och därigenom kränkt eller skadat honom eller henne. Skada innebär både personskada och sakskada och beräkningen av ersättningen regleras genom 5 kap. Skadeståndslagen.[106] En person som på sin webbplats påstått att fem personer (namngivna) gjort sig skyldiga till våldtäkt dömdes för brott mot PUL och skadestånd för kränkning med 5000 kr till två målsägande.[107] En student erhöll 1000 kr i ersättning för kränkning för att ett universitet på ett intranät under mindre än 48 timmars tid hade publicerat en lista med tentamensresultat med hans personnummer.[108] Det framgår av PUL § 49 att i vissa fall kan även böter eller fängelse i högst sex månader, eller om brottet är grovt, till fängelse i högst två år, dömas ut.

3.7 Sammanfattning

PUL syftar till att skydda enskilda personer mot kränkning av den personliga integriteten vid behandling av personuppgifter. Lagen är omfattande och gäller samtliga former av behandling av uppgifter som kan knytas till fysiska personer. PUL grundar sig på dataskyddsdirektivet, vilket har syftet att medlemstaterna ska skydda fysiska personers grundläggande fri- och rättigheter, särskilt rätten till privatliv, i samband med behandling av personuppgifter. Det är den personuppgiftsansvarige som bär ansvaret då en kränkning av en individs personliga integritet skett. För att undvika att denna situation uppstår, ska den personuppgiftsansvarige vidta lämpliga åtgärder för att skydda de personuppgifter som behandlas. Begreppet samtycke är en central del av PUL då det kan avgöra om en behandling är tillåten eller inte.

PUL har anpassat sig till Internet främst i och med lagändringen den 1 januari 2007 vilken innebar att PUL utformades enligt en missbruksmodell till skillnad från en hanteringsmodell. Detta ledde till att vid tillämpning av lagen undersöks om behandlingen av uppgifterna leder till en skada för någons personliga integritet, istället för att titta på själva hanteringen. Förändringen har inneburit att det är tillåtet att hantera personuppgifter i ostrukturerad form via exempelvis e-post så länge behandlingen inte kränker

[105] Blomberg, a.a. s. 125.
[106] Ibid., s. 126.
[107] Helsingborgs tingsrätts dom den 31 januari 2001 i mål nr B 3915-00.
[108] Justitiekanslerns beslut den 28 mars 2003, diarienummer 73-02-42.

den personliga integriteten. De relativt nya reglerna har förenklat vardagligt och oskyldigt användande samtidigt som nya gränsdragningsproblem skapats. All materia på Internet är inte ostrukturerat, snarare tvärtom. Internet kan med sin lättillgänglighet och enkelhet, utan små medel eller planering, sprida en kränkande uppgift och därmed skapa förödande effekter. Trots lagändringen kan idag synliga tillämpningsproblem spåras såsom bristen på riktlinjer för överföring till tredje land och avsaknad av tydliga regler vad gäller nivåer på säkerheten och tillräckliga påföljder.

Vad gäller betydelsen av användarvillkor kan det konstateras att utformningen av villkoren direkt påverkar användaren. Av Googles fall går att sammanfatta att en molntjänstleverantör med stora marknadsandelar kan uppställa användarvillkor utan att ta hänsyn till extraterritoriella lagstiftningar. Hur detta beteende förhåller sig mot EU-rätten går inte idag att säga då beslut inte har fattats i ärendet. Vad som är klart är att; lika illa anpassad PUL är gentemot behandling av personuppgifter i molntjänster, är även dataskyddsdirektivet och resterande av medlemsstaters lagstiftningar på området. Det råder en omodern lagstiftning i EU vilken inte utformades med molntjänster i åtanke. Mer om detta under nästa avsnitt.

4. Skydd av personuppgifter i molntjänster

När användare sparar data med hjälp av program på en server ägd av en molntjänstleverantör, förloras en grad av kontroll över informationen. Det är molntjänstföretaget som har möjlighet att skydda informationen från hackers och interna dataintrång snarare än användaren. Detta innebär att det föreligger en uppenbar risk att placera data i en molntjänst. Ett av de största problemen med molntjänster är att teknikutvecklingen som regel ligger flera år före lagstiftningen.[109] Trots att lagring av användardata på en avlägsen server inte är något nytt fenomen så motiverar den ökade mängden av integritetskränkande brott på Internet en modernisering av lagstiftningen.[110]

4.1 Datainspektionens föreskrift om molntjänster

Datainspektionen utarbetar egna generella föreskrifter, så kallade DIFS[111], för att undanröja oklarheter kring bedömningen och tillämpningen av PUL och de omkringliggande reglerna.[112] Datainspektionen har skrivit en föreskrift om molntjänster och personuppgifter vilken redovisas i detta avsnitt.[113]

Enligt föreskriften är den personuppgiftsansvarige normalt sett den som använder en molntjänst för personuppgiftsbehandling, även om den utförs av molntjänstleverantören eller dess underleverantörer. En molntjänstleverantör, och likaså alla dess underleverantörer som anlitas för behandlingen, är den personuppgiftsansvariges personuppgiftsbiträden.[114] Den personuppgiftsansvarige har följaktligen ansvar för att PUL och andra relevanta lagar efterföljs då denne använder sig av en molntjänst.[115] Enligt datainspektionen ska denne vidta ett antal säkerhetsåtgärder. För det första

---

[109] Privacy Rights Clearinghouse, *The Privacy Implications of Cloud Computing*, http://www.privacyrights.org/ar/cloud-computing.htm (2012-05-14, kl. 14.00).
[110] Gellman, Robert, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, The World Privacy Forum, 2009-02-23, http://www.worldprivacyforum.org/cloudprivacy.html (2012-06-19, kl. 14.30).
[111] Förkortning av: datainspektionens föreskrifter.
[112] T.ex. myndighetsspecifika registerförfattningar och offentlighets- och sekretesslagen.
[113] Datainspektionen, *Molntjänster och Personuppgiftslagen*, 2011.
[114] Ibid., s. 1.
[115] T.ex. myndighetsspecifika registerförfattningar och Offentlighets- och Sekretesslagen (2009:400).

bör den personuppgiftsansvarige göra en laglighetsbedömning innan en molntjänst används. En sådan bedömning innebär en uppskattning av om den personuppgiftsbehandling molntjänstleverantören ska utföra kommer att vara tillåten enligt PUL.[116] Den andra säkerhetsåtgärden är att kontrollera att standardavtalet innehåller villkor i överensstämmelse med PUL och andra relevanta regler. Den personuppgiftsansvarige bör ta ställning till om det finns risk för att personuppgifter kan komma att behandlas för andra ändamål än de ursprungliga. Den tredje säkerhetsåtgärden är att den personuppgiftsansvarige bör bedöma om molntjänstleverantören kan komma att lämna över personuppgifter till ett land utanför EU och EES, och i så fall om en sådan överföring har stöd enligt PUL[117].

Personuppgifter, som överförs via Internet eller andra öppna nät, ska enligt datainspektionen skyddas på något sätt, exempelvis genom kryptering, eftersom de lätt kan råka ut för avlyssning, förvanskning och ändring. Beroende på känsligheten av personuppgifterna som behandlas ställs högre krav på säkerhet. Vad gäller e-postsystem, föreligger ett antal grundläggande säkerhetsbrister i de kommunikationsprotokoll som ligger till grund för systemet. När ett e-postmeddelande skickas kan det passera och lagras på ett antal servrar längs vägen. Ett mottaget e-postmeddelande ligger kvar på e-postserverarna och en kopia av det skickade e-postmeddelandet ligger vanligen kvar hos avsändaren. Om informationen i e-postmeddelandet är oskyddad (exempelvis okrypterad), finns det risk att obehöriga kan ta del av informationen vid var och en av dessa servrar.[118] I ett beslut bedömde datainspektionen att Socialnämnden i Nacka inte vidtagit tillräckliga säkerhetsåtgärder då de behandlat känsliga personuppgifter i sitt e-postsystem. Uppgifter av denna typ får enbart lämnas ut via öppna nät till identifierade användare vars identitet är säkerställd med en teknisk funktion som kryptering, engångslösenord eller motsvarande, enligt datainspektionen.[119]

Den personuppgiftsansvarige bör även bedöma vilka säkerhetsåtgärder som kan komma att bli nödvändiga för att skydda personuppgifter på ett sätt som motsvarar PUL och andra relevanta regler. Detta bör upprättas i villkoren i personuppgiftsbiträdesavtalet med molnleverantören. I de fall ett avtal inte tillför något till integritetsskyddet, t.ex. när personuppgiftsbiträdet endast lagrar material som är identiskt med sådant som lagligen publicerats på Internet, föreligger inget tvång på att upprätta ett sådant avtal.[120] I annat fall skall personuppgiftsbiträdesavtalet bland annat innehålla villkor att

---

[116] Datainspektionen, *Molntjänster och Personuppgiftslagen*, a.a. s. 2.
[117] Ibid., s. 2.
[118] Datainspektionens beslut i ärendet: Tillsyn enligt personuppgiftslagen (1998:204) – Salems kommunstyrelse, 2011-09-28, diarienummer 263-2011, s. 17.
[119] Datainspektionens beslut i ärendet: Beslut efter tillsyn enligt personuppgiftslagen (1998:204), 2006-12-12, diarienummer 1082-2006.
[120] Datainspektionen, *Molntjänster och Personuppgiftslagen*, a.a. s. 3.

personuppgiftsbiträdet ska vara skyldigt att behandla personuppgifter i enlighet med den personuppgiftsansvariges instruktioner. Vidare ska den personuppgiftsansvarige ha kännedom om vilka andra personuppgiftsbiträden som kan komma att behandla personuppgifterna. Personuppgiftsbiträdet ska även säkerställa att den personuppgiftsansvarige har möjlighet att följa upp att personuppgiftsbiträden lever upp till den personuppgiftsansvariges krav på personuppgiftsbehandlingen och verkligen vidtar lämpliga säkerhetsåtgärder. Det ska även finnas tekniska och praktiska förutsättningar för att utreda misstankar om att någon hos den personuppgiftsansvarige eller hos något personuppgiftsbiträde haft obehörig åtkomst till personuppgifterna.[121] Vid avtalets upphörande ska parterna vara medvetna om vilka åtgärder som ska vidtas så att personuppgiftsbiträdet inte har åtkomst till personuppgifterna därefter. I de fall personuppgifter behandlas av personuppgiftsbiträden i ett land utanför EU och EES är det upp till den personuppgiftsansvarige att se till att PUL efterföljs.[122]

Slutligen bör den personuppgiftsansvarige även genomföra en risk- och sårbarhetsbedömning för att bedöma om det är lämpligt att anlita den tänkte molntjänstleverantören. Det är risken för att behandlingen ska leda till att någons personliga integritet ska skadas som ska bedömas. De omständigheter som bedöms är antalet personer de behandlade uppgifterna avser, mängden uppgifter som behandlas om varje person, känsligheten hos de behandlade personuppgifterna och om personuppgifterna kan struktureras eller inte.[123] När det gäller känsliga personuppgifter, brottsuppgifter och sekretesskyddade uppgifter kräver datainspektionen att det ska finnas stark autentisering vid överföringen i öppet nät då det kan leda till att uppgifterna överförs till tredje land. Vidare bör den personuppgiftsansvarige utföra regelbundna kontroller och inneha kontinuerlig vetskap om vem som har haft åtkomst till vilka uppgifter.[124]

Datainspektionen har i egenskap av tillsynsmyndighet på eget initiativ utfört inspektioner av felaktigheter vid användande av molntjänster. Under slutet av 2011 granskades två kommuner och ett företag i Sverige; Enköpings kommunstyrelse, Salems kommunstyrelse och Brevo AB. Dessa tre organisationer fick underkänt av datainspektionen i sin behandling av personuppgifter.[125] Nedan redogörs för dessa tillsynsbeslut.

[121] Ibid., s. 3.
[122] Ibid., s. 3.
[123] Ibid., s. 2.
[124] Ibid., s. 2-3.
[125] Ilijason, Robert, *PUL-stormen hotar molnet*, TechWorld, vol/nr: 2012: 1-2, 4.

4.1.1 Datainspektionens beslut i tillsynsärendet: Enköpings kommunstyrelses användning av molntjänsten Dropbox

Enköpings kommunstyrelse använde under datainspektionens tillsyn en gratisversion av Dropbox för att förmedla kallelser, handlingar och protokoll till tjänstemän samt ledamöter i kommunstyrelsen och arbetsutskotten inför nämndesammanträden. Sammanlagt använde sig 22 personer av molntjänsten. Samma handlingar som fanns på Dropboxkontot publicerades även på kommunens webbplats och dokument som bedömdes som olämpliga att läggas upp på webbplatsen, lades inte heller upp på Dropbox.[126]

I beslutet från datainspektionen konstaterades att Enköpings kommunstyrelse var personuppgiftsansvarig för den personuppgiftsbehandling som deras anställda utfört i tjänsten.[127] Vidare fastställdes att både Dropbox Inc. och dess underleverantörer, som behandlat personuppgifter för kommunstyrelsens räkning, var personuppgiftsbiträden till kommunstyrelsen. I egenskap av personuppgiftsansvarig fastställdes det att kommunstyrelsen hade det fulla ansvaret för att behandlingen av personuppgifter skulle utföras i enlighet med dataskyddsbestämmelserna i svensk lag, vilket inte förändrades av att personuppgiftsbehandlingen hade utförts av personuppgiftsbiträden.[128] Datainspektionen förelade kommunstyrelsen att ge tydliga instruktioner till sina anställa om under vilka förutsättningar kommunstyrelsen tillåter lagring av arbetsmaterial och annat material som innehåller personuppgifter i Dropbox. Slutligen förelades även kommunstyrelsen att göra en risk- och sårbarhetsanalys av behandlingen för att bedöma under vilka förutsättningar behandling av personuppgifter genom lagring dokument är tillåten enligt PUL.[129]

4.1.2 Datainspektionens beslut i tillsynsärendet: Brevo AB

Brevo är en digital brevlåda som företag och myndigheter kan använda för att distribuera brev. För att brev ska kunna skickas har avsändare samt mottagare skapat ett konto hos Brevo. För denna tjänst har Brevo använt sig

[126] Datainspektionens beslut i ärendet: Tillsyn enligt personuppgiftslagen (1998:204) – Enköpings kommunstyrelses användning av molntjänsten Dropbox, 2011-09-28, diarienummer 256-2011, s. 2.
[127] Ibid., s. 1.
[128] Ibid., s. 1.
[129] Ibid., s. 1.

av Windows Azure, en av Microsofts molntjänster. De personuppgifter som Brevo samlade in och lagrade om privatpersoner som använde tjänsten var personnummer, för- och efternamn, e-postadress och, i vissa fall mobiltelefonnummer.[130]

I beslutet från datainspektionen konstaterades det att Brevo var personuppgiftsansvarig. Brevo ansågs inte ha upprättat ett fullständigt personuppgiftsbiträdesavtal eftersom det av avtalet framkom att andra företag än Microsoft skulle kunna komma att behandla personuppgifterna. Brevo ansågs med andra ord inte ha kunskap om vilka bolag som behandlade personuppgifterna för företagets räkning.[131] Datainspektionen framhöll i sitt beslut att personuppgiftsbiträdesavtalet var otydligt och ensidigt vilket möjliggjorde för Microsoft att ensidigt förändra användarvillkoren, vilket kunde medföra stora risker för den personuppgiftsansvarige.[132]

4.1.3 Datainspektionens beslut i tillsynsärendet: Salems kommunstyrelse

Datainspektionens granskning av Salems kommunstyrelse baserades på personuppgiftsbiträdesavtalet mellan Google Ireland Ldt och styrelsen för användandet av Google Apps. Molntjänsten skulle sköta behandlingen av personuppgifter vid hanteringen av e-post, kalender och chat samtidigt som kommunstyrelsen var personuppgiftsansvarig.[133] Datainspektionen kom fram till att kommunstyrelsen inte hade kunskap om vilka bolag inom Google-koncernen som behandlade uppgifterna för deras räkning. Andra bolag än Google Ireland Ldt hade möjlighet att behandla uppgifterna, vilket gjorde att samtliga bolag inom Google-koncernen bedömdes vara personuppgiftsbiträden.[134] Enligt avtalet lagrades uppgifterna inom EU och EES eller inom USA där Safe Harbor-principerna gäller, eftersom Google Ireland Ldt var ansluten till dessa. Personuppgifterna lagrades på flera ställen, och enligt datainspektionen kunde uppgifterna behandlas även av andra bolag i USA, för vilka det inte kunde fastställas om de var anslutna till Safe Harbor-principerna.[135]

Datainspektionen förelade kommunstyrelsen att antingen teckna avtal med varje bolag inom Google-koncernen som behandlade personuppgifter för kommunstyrelsens räkning, eller genom att i ett avtal ge Google Ireland Ltd

---

[130] Datainspektionens beslut i ärendet: Tillsyn enligt personuppgiftslagen (1998:204) – Brevo AB, 2011-09-28, diarienummer 574-2011, s. 2.
[131] Ibid., s. 1.
[132] Ibid., s. 7.
[133] Datainspektionens beslut i ärendet: Tillsyn enligt personuppgiftslagen (1998:204) – Salems kommunstyrelse, 2011-09-28, diarienummer 263-2011, s. 3-4.
[134] Ibid., s. 9.
[135] Ibid. s. 17.

eller Google Inc. mandat att ingå ett avtal med underbiträden, där det föreskrivs att varje personuppgiftsbiträde har samma skyldigheter som det personuppgiftsbiträde som kommunstyrelsen ingår avtal med. Vidare förelade datainspektionen kommunstyrelsen att ha kännedom om vilka personuppgiftsbiträden som behandlar personuppgifterna.[136]

Sammantaget fastställde datainspektionen att personuppgiftsbiträdesavtalet inte levde upp till kraven enligt PUL då villkoren i avtalet inte var urskiljbara från övriga villkor mellan parterna. Villkoren kunde vidare ensidigt förändras av personuppgiftsbiträdet. Kommunstyrelsen ansågs inte heller kunna säkerställa att åtkomsten till personuppgifterna inte längre förelåg för personuppgiftsbiträdet efter avtalets upphörande. Avtalet säkerställde inte heller att svensk lagstiftning skulle tillämpas samt att det vid misstanke om obehörig åtkomst av personuppgifterna fanns tekniska och praktiska förutsättningar att utreda detta. Kommunstyrelsen kunde inte säkerställa att Google Ireland Ldt endast behandlade personuppgifterna i enlighet med kommunstyrelsens instruktioner.[137]

4.2 Sammanfattning

Gemensamt för samtliga tre redogjorda tillsynsbesluten är att de granskade organisationerna använde sig av några av de vanligaste molntjänstleverantörerna; Dropbox, Google och Microsoft. Datainspektionen kritiserade att Brevo och Salem inte hade upprättat ett korrekt personuppgiftsavtal med molntjänstleverantörerna samt att de inte hade fullständig kunskap om säkerhetsnivån. Enköpings kommunstyrelse hade i princip liknande brister men kom undan med ett föreläggande om att skriva tydligare instruktioner istället för föreläggande om att rätta till bristerna.[138]

I de tre granskningarna har datainspektionen tydligt visat att det föreligger en medvetenhet om PULs brister i förhållande till molntjänstanvändande. I samtliga tillsynsärenden har datainspektionen skrivit att dagens dataskyddslagstiftning är svår att förena med det som vi idag kallar för molntjänster. Detta på grund av att PUL utgår från att det är den personuppgiftsansvarige som är den starke, bestämmande aktören som kan instruera och kontrollera vad dennes personuppgiftsbiträde gör. I praktiken ser det istället ut som så att personuppgiftsbiträden erbjuder en tjänst med tillhörande användarvillkor, vilka de sällan är villiga att ändra. Molntjänstleverantörerna går alltså sin egen väg och använder sig av egenkomponerade användarvillkor. Detta är en situation som inte

[136] Ibid., s. 12.
[137] Ibid., s. 10-16.
[138] *Risker med otydliga avtal för molntjänster*, Mitt i Juridiken, 2011-11-30.

lagstiftaren hade i åtanke då PUL skrevs. Det är ett generellt problem för den personuppgiftsansvarige att molntjänstleverantören inte sällan är den starkare parten som dikterar användarvillkor. Då PUL inte skrevs på det sättet att den personuppgiftsansvarige skulle vara den svagare parten, leder detta till tillämpningsproblem. PUL ställer ett antal krav på den personuppgiftsansvarige vilken denne har svårt att genomföra i praktiken på grund av molntjänstleverantören ofta inte är samarbetsvillig eller ogärna vill bli styrd av utländska regleringar. Den personuppgiftsansvarige behöver kunna kliva in hos personuppgiftsbiträdet och kontrollera om säkerheten är tillräcklig, och detta är något som inte sällan vägras av molntjänstleverantörer.

Trots att datainspektionen inser problemet med bristerna i PUL i förhållande till behandling av personuppgifter i molntjänster, visar de tre granskningsbesluten att företag som använder sig av molntjänster anses bära det fulla ansvaret för brister i användaravtal, trots att de inte har någon direkt möjlighet till att påverka dess innehåll. I de tre utredningarna gav datainspektionen de personuppgiftsansvariga fullt ansvar för att behandlingarna av personuppgifterna skulle utföras i enlighet med svensk lag. Det förändrades inte av att personuppgiftsbehandlingen hade utförts av personuppgiftsbiträden. Detta trots att det uttryckligen står i datainspektionens föreskrift att personuppgiftsbiträdet har en skyldighet att säkerställa att den personuppgiftsansvarige har möjlighet att följa upp att personuppgiftsbiträdet lever upp till den personuppgiftsansvariges krav på personuppgiftsbehandlingen. Jag tolkar datainspektionens föreskrift som så, att molntjänstleverantörer har ett ansvar i behandlingen av personuppgifter. Datainspektionen har dock klargjort i sina tre tillsynsgranskningar att så inte är fallet i praktiken.

5. EU-kommissionens förslag om en dataskyddsförordning[139]

Den 25 januari 2012 presenterade EU-kommissionen ett förslag om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän dataskyddsförordning). Förslaget innebär en genomgripande reform av EU:s regler om skydd för personuppgifter och innebär att dataskyddsdirektivet, och därmed PUL kommer att ersättas av en ny allmän dataskyddsförordning.[140] Motivet bakom förslaget är bland annat att det skett förändringar i teknik och hur tekniken används sedan 1995, då den nuvarande regleringen infördes. Kommissionen har även framhållit att medlemsstaterna har genomfört reglerna på olika sätt och mot denna bakgrund är syftet med förslaget att harmonisera, modernisera och effektivisera reglerna för skyddet av personuppgifter. Regleringen föreslås få formen av en förordning vilket innebär direkt tillämpning i medlemsländerna.[141] Grundvalen för förordningen är att skydda den personliga integriteten. EU-kommissionens vice president Vivianne Reding[142] sade vid presentationen av förslaget:

> "17 years ago less than 1% of Europeans used the Internet. Today, vast amounts of personal data are transferred and exchanged, across continents and around the globe in fractions of seconds. The protection of personal data is a fundamental right for all Europeans, but citizens do not always feel in full control of their personal data. My proposals will help build trust in online services because people will be better informed about their rights and in more control of their information. The reform will accomplish this while making life easier and less costly for businesses. A strong, clear and uniform legal framework at EU level will help to unleash the potential of the Digital Single Market and foster economic growth, innovation and job creation."[143]

---

[139] Översättning av: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard of the processing of personal data and on the free movement of such data.
[140] Justitiedepartementet, *Faktapromemoria 2011/12:FPM117 Allmän dataskyddsförordning*, s. 1.
[141] Ibid., s. 1.
[142] Vivianne Reding är ledamot i Europeiska kommissionen sedan 1999.
[143] European Commission, *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses*, 2012-01-25, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46 (2012-05-

Förslaget utökar den personuppgiftsansvariges roll jämfört med dataskyddsdirektivet då den registrerade ges ett antal rättigheter vilka inte föreligger idag. Den registrerade ska bland annat informeras om vilka uppgifter som behandlas, ändamålet med behandlingen, hur länge uppgifterna ska lagras, få möjlighet att flytta data från en tjänsteleverantör till en annan och även kunna få del av en komplett kopia av alla personuppgifter på ett strukturerat sätt i elektroniskt format.[144] Den personuppgiftsansvarige ska även se till att behandlingen endast avser personuppgifter som är nödvändiga i förhållande till syftet med behandlingen. Vidare ska den personuppgiftsansvarige dokumentera vilken behandling som genomförs, vilken efter begäran ska göras tillgänglig för tillsynsmyndigheten. Den personuppgiftsansvarige ska skydda uppgifterna som behandlas och dessutom, om möjligt inom 24 timmar, underrätta en tillsynsmyndighet om ett dataintrång har ägt rum.[145]

5.1 Personuppgiftsbehandling som omfattas av förslaget

Förordningen föreslås vara tillämplig på all helt eller delvis automatiserad behandling av personuppgifter, samt på manuell behandling av personuppgifter om uppgifterna ingår eller är avsedda att ingå i en strukturerad samling av personuppgifter. Förslaget är tillämpligt på behandling av personuppgifter som utförs av en personuppgiftsansvarig som är etablerad inom EU, samt på behandling av uppgifter om en enskild som är bosatt inom EU om behandlingen avser antingen erbjudande om varor eller tjänster till den enskilde eller övervakning av den enskildes beteende.[146]

I vissa delar har medlemstaterna befogenhet att inskränka vissa rättigheter och skyldigheter genom nationell lagstiftning, t.ex. när det gäller reglering av nationella tillsynsmyndigheter och påföljder för överträdelser, så länge de är nödvändiga och proportionerliga i förhållande till ändamålet.[147] Medlemstaterna ges möjlighet att lagstifta om undantag från vissa av bestämmelserna för behandling som sker för t.ex. journalistiska ändamål, för konstnärligt eller litterärt skapande, hälsoändamål och forskningsändamål. Dessa möjligheter till undantag är framtagna för att det ska föreligga en balans mellan skyddet för personuppgifter och

---

24, kl. 10.30).
[144] Proposal for General Data Protection Regulation, s. 8.
[145] Ibid., s. 8-9.
[146] Konstitutionsutskottet, *Utlåtande 2011/12:KU25 EU-förslag om allmän uppgiftsskyddsförordning*, s. 14.
[147] Ibid., s. 5.

yttrandefriheten.[148]

5.2 Definitionen av den registrerades samtycke

Definitionen av samtycke enligt förslaget innebär att det i de flesta fall måste vara uttryckligt för att det ska anses giltigt. Denna typ av samtycke kallas ”opt-in” samtycke.[149] Den personuppgiftsansvarige ska ha tydliga och lättillgängliga riktlinjer och vara skyldig att ge klar och tydlig information till den registrerade vad gäller behandlingen av personuppgifter för att denne ska kunna ge ett giltigt samtycke.[150] Behandlingen av personuppgifter ska ske på ett öppet sätt och bevisbördan för att ett samtycke från den registrerade föreligger ska ligga på den personuppgiftsansvarige.[151]

Samtycket ska enligt förslaget vara lätt att ta bort, vilket innebär en rätt för den registrerade att få sina uppgifter raderade, samtidigt som den personuppgiftsansvarige utan dröjsmål ska vidta rimliga åtgärder för att informera dem som uppgifterna spridits till att den registrerade vill bli glömd.[152]

5.3 Dataskyddsförordningens territoriella tillämpningsområde

När det gäller dataskyddsförordningens territoriella tillämpningsområde anges i förslaget att förordningen är tillämplig på behandling av personuppgifter som utförs av en personuppgiftsansvarig, som är etablerad inom EU samt på behandling av uppgifter om en enskild som är bosatt inom EU om behandlingen avser antingen erbjudande om varor eller tjänster till den enskilde eller övervakning av den enskildes beteende. Detta innebär att dataskyddsregleringens tillämpningsområde utökas till att även omfatta uppgiftsbehandling som sker utanför EU så länge behandlingen utförs av företag som t.ex. erbjuder varor eller tjänster till EU-medborgare.[153]

---

[148] Justitiedepartementet, a.a. s. 8.
[149] Proposal for General Data Protection Regulation, s. 4.
[150] Sjögren, Per-Anders, *Rätt att radera uppgifter om privatlivet från internet*, Riksdag & Parlament, s. 12.
[151] Justitiedepartementet, a.a. s. 5.
[152] Ibid., s. 5.
[153] Konstitutionsutskottet, a.a. s. 14.

5.4 Överföring av personuppgifter till tredje land

Vad gäller överföring av personuppgifter till tredje land eller en internationell organisation ska mottagaren uppnå en adekvat skyddsnivå för uppgifterna enligt dataskyddsförordningen.[154] Förslaget speglar EG-domstolens förhandsavgörande i det så kallade Bodil-målet där det uttalades att bedömningen av huruvida skyddsnivån är adekvat skall ske på grundval av alla de förhållanden som har samband med en överföring eller en grupp av överföringar av uppgifter. Uppgiftens art, den eller de avsedda behandlingarnas ändamål och varaktighet, ursprungslandet och det slutliga bestämmelselandet, de allmänna respektive särskilda rättsregler som gäller i ifrågavarande tredje land liksom de regler för yrkesverksamhet och säkerhet som gäller där, ska beaktas.[155]

Huruvida överföring av uppgifter till tredje land föreligger då personuppgifter läggs ut på en webbplats framgår inte direkt av förslaget. EG-domstolen klargjorde den frågan i förhållande till dataskyddsdirektivet då Göta Hovrätt, i samma mål som ovan, ställde frågan om det förelåg en överföring av uppgifter till tredje land när en person som befinner sig i en medlemsstat lägger ut personuppgifter på en webbsida som är lagrad hos en fysisk eller juridisk person som hyser den webbplats där webbsidan kan läsas och som är etablerad i samma medlemsstat eller i en annan medlemsstat, varvid uppgifterna blir åtkomliga för alla som kopplat upp sig på Internet, inklusive personer i tredje land.[156] EG-domstolen konstaterade att uppgifter på Internet kan läsas av ett obestämt antal personer vilka befinner sig på en mängd olika geografiska platser.[157] Trots detta fastslog domstolen att det inte förelåg någon överföring till tredje land i målet. Hänsyn togs till dels det stadium på vilket Internets utveckling befann sig vid den tidpunkt då direktivet utarbetades, och dels till att inga kriterier anges i direktivet vilka är tillämpliga på Internetanvändning. Av dessa skäl drog domstolen slutsatsen att det inte kan presumeras att gemenskapslagstiftaren hade för avsikt att med tanke på framtiden låta ett utläggande av uppgifter på en webbsida omfattas av begreppet ”överföring av uppgifter till tredje land”, även om dessa på detta sätt blir åtkomliga för sådana personer i tredje land som har de tekniska möjligheterna att få tillgång till hemsidan.[158]

Det går inte att utläsa ur förslagets form idag huruvida situationen som

---

[154] Ibid., s. 7.
[155] EG-domstolens avgörande den 6 november 2003 i mål C-101/01, p. 8.2 i domskälen.
[156] Ibid., p. 52.
[157] Ibid., p. 58.
[158] Ibid., p. 4, 63, 64, 68, 71.

beskrivits ovan är att anses som en överföring av personuppgifter till tredje land. Det som går att konstatera är att dataskyddsförordningen onekligen har kriterier för Internetanvändande och i de fall den går igenom kommer gemenskapslagstiftaren med största sannolikhet ha Internetanvändande i åtanke. En mer genomgående diskussion om detta under avsnitt 6.2.

5.5 Hanteringsmodell

Missbruksregeln i PUL § 5 ska inte gälla enligt förslaget. Regeln är beskriven ovan och innebär i korthet att vardaglig behandling av material vilken inte kan leda till kränkning av personliga integriteten ska vara tillåten så länge uppgifterna är ostrukturerade. Detta innebär att personuppgiftsbehandling, såsom publicering på webbplatser m.m. kommer att omfattas av förslagets samtliga regler, t.ex. skyldighet för den registreringsansvarige att informera, dokumentera ändamål, rätt för den enskilde att bli bortglömd och göra invändning. Förslaget ger dock medlemsstaterna möjlighet att göra undantag för behandling som sker uteslutande för journalistiska, konstnärliga och litterära ändamål, vilket motsvarar de undantag som föreligger i PUL till skydd för tryck- och yttrandefriheten.[159]

David Törngren vid justitiedepartementet, som medverkat vid förhandlingarna om förordningen, menade vid en telefonintervju att det är svårt att utröna i dagsläget hur möjligheterna kommer att se ut för att utnyttja undantagen för bland annat journalistiska ändamål. Törngren framhöll vidare att förslaget kommer att ha formen av en förordning, vilket innebär att medlemsstaternas bestämmanderätt minskar och därmed även möjligheterna för nationella lösningar i jämförelse med ett direktiv. Det är ännu inte bestämt hur omfattande medlemsstaternas bestämmanderätt kommer att vara, och diskussioner och förhandlingar pågår i skrivande stund. Törngren framhöll att det är ett komplicerat lagområde och det kommer att ta tid innan ett beslut fattas.[160]

5.6 Tillsyn

Förslaget anger att tillsynsmyndigheterna i varje medlemsland (datainspektionen i Sverige) ska vara oberoende och utöva tillsyn över att förordningen följs. Tillsynsmyndigheterna har enligt förslaget en skyldighet att pröva klagomål om uppgiftsbehandling och ska väcka talan i domstol vid överträdelser mot bestämmelserna i förordningen. I förslaget ingår även en

[159] Proposal for General Data Protection Regulation, s. 7.
[160] Intervju med David Törngren vid justitiedepartementet, 2012-04-27, kl. 10.00.

befogenhet för de nationella tillsynsmyndigheterna att besluta om administrativa sanktionsavgifter. Tillsynsmyndigheterna förelås samarbeta på ett sätt så att förordningen tillämpas på ett konsekvent sätt i hela EU genom införandet av en europeisk dataskyddsstyrelse. Respektive nationell tillsynsmyndighet är skyldig att samråda med dataskyddsstyrelsen innan en åtgärd med effekt i flera medlemsstater kan tas.[161]

Vad gäller rättsmedel, ansvar och sanktioner gäller i princip samma förhållanden som i nuvarande lagstiftning och förslaget slår fast att enskilda, organisationer, sammanslutningar, juridiska personer ska ha rätt att klaga hos en nationell tillsynsmyndighet om de anser att en behandling av personuppgifter inte följt förordningen. I likhet med vad som redan gäller ska den enskilde även ha rätt att väcka talan i domstol mot en personuppgiftsansvarig. I det fall en enskild drabbas av en skada på grund av en otillåten behandling av personuppgifter ska han eller hon ha rätt till skadestånd från den som är ansvarig för behandlingen. Det är medlemsstaterna som bestämmer de sanktioner som ska komma i fråga vid överträdelser av förordningens bestämmelser. Sanktionerna har krav på sig att vara effektiva, proportionerliga och avskräckande. I förslaget ges nationella tillsynsmyndigheter en rätt att besluta om administrativa avgifter, vilka ska kunna uppgå till en miljon kronor, eller två procent av ett företags globala omsättning, vid de allvarligaste överträdelserna av förordningens bestämmelser.[162]

5.7 Sammanfattning

EU-kommissionens förslag innebär en klar förstärkning av den enskildes rättigheter, samtidigt som skyldigheterna för den personuppgiftsansvarige avsevärt ökar. Den enskilde har enligt förslaget bland annat rätt till insyn och rätt att veta ändamålet med behandlingen, rätt att bli glömd och rätt att invända mot uppgiftsbehandling. Den personuppgiftsansvarige är samtidigt enligt förslaget skyldig, utöver det som i stort sett gäller redan enligt dataskyddsdirektivet, att behandla personuppgifter på ett öppet sätt, bevisa att samtycke föreligger, dokumentera och informera den enskilde om behandlingen. Sanktionerna enligt förslaget är högre och EU-kommissionen sätter högre krav på tillsynsmyndigheterna än dagens dataskyddsdirektiv. Kommissionen föreslår vidare att hanteringsregler ska tillämpas även på sådan behandling som sker i ostrukturerad form, dvs. i löpande text på Internet eller sociala medier, vilket innebär att överväganden och planering kommer behövs vid ”vardaglig” behandling. Införandet av en hanteringsmodell skiljer sig från dagens utformning och effekterna av denna

[161] Proposal for General Data Protection Regulation, s. 29-30.
[162] Ibid., s. 29-30.

del i förslaget är svåra att förutse. Hur omfattande bestämmanderätt medlemsstaterna kommer att ges, blir i mångt och mycket vara avgörande.

Huruvida EG-domstolen bedömer en publicering av personuppgifter på en webbplats utgör en överföring till tredje land enligt dataskyddsförordningen är något som inte går att fastställa i dagsläget. Det kan dock konstateras att EG-domstolens två domskäl i Bodil-målet, vilka baserades på Internets utveckling samt frånvaron att kriterier för Internetanvändning, svårligen kan appliceras på förslaget, vilket i mångt och mycket har framgenererats till följd av Internets utveckling. Ytterligare kan stadgas att förordningsförslaget utökade territoriella tillämplighet gör att förslaget troligtvis ändå blir tillämpligt i de fall personuppgifter tillhörande EU-medborgare läggs ut på en webbplats.

6. Förslaget respektive PULs fördelar och nackdelar

I inledningen angavs att syftet med uppsatsen var att undersöka skyddet av personuppgifter vid anlitandet av molntjänster i dag samt vid en eventuell framtida lagförändring. Undersökningen har baserats på de nuvarande svenska reglerna, PUL, samt EU-kommissionens förslag om ny dataskyddsförordning. Eftersom molntjänster förekommer i åtskilliga och varierande former, förekommer skilda säkerhetsproblem beroende på vilken typ av molntjänst som är för handen och i vilket syfte tjänsten används. Frågeställningarna har besvarats med en allmän syn på molntjänster, utan hänsyn till specifika applikationer och egenskaper. Detta komplicerade område leder till att det är svårt att ge raka svar på hur en tillämpning skulle komma att bli i och med förordningsförslaget. I detta avslutande avsnitt sammanfattas de viktigaste slutsatserna. Som angavs i inledningen är det ett antal problem som kommer i förgrunden när det gäller skyddet för den personliga integriteten vid molntjänstanvändande: lagstiftningsform, territoriell tillämpning, överföring av personuppgifter till tredje land, krav på samtycke, molntjänsters användarvillkor, den personuppgiftsansvariges roll, missbruksregeln och hanteringsmodellen samt tillsyn vid överträdelse.

6.1 Lagstiftningsform

Förslagets form av en direktverkande förordning ger andra premisser jämfört med om förslaget skulle ha formen av ett direktiv. En förordning gäller omedelbart för alla medborgare, företag och medlemsländer i EU, och innebär att alla kan åberopa den direkt vid domstol, och domstolen måste tillämpa den.[163] En lagstiftning i form av ett direktiv skulle istället innebära att regelverket skulle införas i alla medlemsstater vilka skulle haft ett fortsatt stort ansvar, dels genom nationella lagstiftande församlingar och dels genom nationella dataskyddsmyndigheter. Erfarenheterna från den ojämna och bristfälliga implementeringen av dataskyddsdirektivet var en av de främsta orsakerna till att EU-kommissionen kom med sitt förslag. Av detta skäl kan det tyckas svårt att se att ett nytt direktiv skulle ha större genomslagskraft jämfört med det som varit gällande i 16 år.

Vad gäller skydd av personuppgifter inom molntjänster är det särskilt viktigt att en synkroniserad och harmoniserad lagstiftning föreligger då

[163] Artikel 288 i Lissabonfördraget preciserar att förordningar är direkt tillämpbara i medlemsstaterna. EU-domstolen preciserar i domen i målet Politi av den 14 december 1971 att det rör sig om en fullständig direkt effekt.

leverantörerna sällan verkar på nationell basis eller är lokaliserade på en specifik fast plats. En förordning skulle därmed underlätta och klargöra vad som är tillåtet och otillåtet för både användaren och molntjänstleverantören. De senare skulle slippa att oroa sig för olika juridiska krav i olika medlemsstater. Regler i form av en förordning skulle samtidigt inte kunna ändras eller anpassas till medlemsländernas olika rätts- och kulturtraditioner. I relation till molntjänster är detta något som är av mindre betydelse, då dessa verkar på internationell basis.

Förslagets utformning som en förordning leder att makt skjuts från medlemsländerna till EU-kommissionen. Sverige skulle därmed förlora det handlingsutrymme som ett direktiv ger i samband med implementering. Detta gör att förslaget, vilket skyddar en mängd integritetsskyddsintressen framför yttrandefriheten, kan åsidosätta Sveriges offentlighetsprincip. Beslut som enligt svensk grundlag ska fattas av riksdagen kommer att förflyttas till kommissionen. Vid presentationen av förordningsförslaget anförde kommissionen att de föreslagna bestämmelserna till skydd för integriteten inte ska äga företräde före grundläggande yttrandefrihetsintressen. Medlemsstaterna får förvisso rätt att föreskriva undantag för tillämpning av förordningsföreskrifterna med hänvisning till yttrandefrihet, dvs. en rätt att tillskapa undantag för behandling som sker uteslutande för journalistiska, konstnärliga och litterära ändamål. Dock ska det inte glömmas att dylika nu gällande regler i respektive land inte kommer att gälla om förslaget träder i kraft om inte yttrandefriheten är lagstadgad, som i Sverige, i en särskild lag från den som kommer ersättas. Det tycks heller inte framgå i förslagstexten hur dessa avvägningar ska göras vilket gör att det finns utrymme för en mängd olika tolkningar. Det framstår som ytterst oklart hur denna rätt att skydda offentlighetsprincipen kommer att ske samt hur stor bestämmanderätt medlemsstaterna verkligen kommer att ha. Förslagstexten och förarbetena är inte uttömmande och öppnar onekligen upp för ett tolkningsutrymme.

Den 29 mars 2012 skickade riksdagen ett s.k. motiverat yttrande till Europaparlamentets, rådets och kommissionens ordförande där det stadgades att Sveriges riksdag anser att förslaget om allmän uppgiftsskydd inte är förenlig med subsidiaritetsprincipen.[164] I dagsläget har Belgien, Tyskland, Italien och Frankrike skrivit varsitt motiverat yttrande innehållande invändningar till förslaget, vilka i stort hävdar att EU får en alltför omfattande bestämmanderätt i och med förslaget.[165] Hur utgången blir av dessa yttranden är idag oklart, men det går att konstatera att området berör många och en framtida ny lagstiftning, särskilt i form av en förordning, kommer påverka många parter och medlemsländer.

[164] Riksdagsskrivelse 2011/12:178.
[165] Interparliamentary Exchange, a.a.

6.2 Territoriell tillämpning

Vad gäller behandling av personuppgifter i molntjänster är en primär fråga vilken lag som är tillämplig. PUL stadgar att det är utrustningen som avgör tillämplig lag vilket gör att i de fall utrustningen befinner sig i Sverige är PUL tillämplig. Dataskyddsförordningen stadgar att även uppgiftsbehandling vilken sker utanför EU som berör EU-medborgare ingår i förordningens territoriella tillämpningsområde. Förslagets utökning av det territoriella tillämpningsområdet förenklar och förtydligar villkoren för molntjänstanvändare inom EU då tillämpningen blir mer enhetlig. PULs utformning gör att flertalet företag undkommer reglerna genom att flytta information, servar eller företag utomlands, trots att uppgifterna rör svenska konsumenter.[166] Det föreligger med andra ord en lucka i PUL vilken med förordningsförslagets utformning troligtvis kommer att försvinna. Rättssäkerheten vad gäller tillämplig lag ser därmed ut att höjas i och med bruk av dataskyddsförordningen jämfört med PUL.

Förslagets del om att reglerna ska tillämpas även på behandling av personuppgifter som utförs av en personuppgiftsansvarig som är etablerad inom EU samt på behandling av uppgifter om en enskild som är bosatt inom EU, är något som otvivelaktigt kommer att leda till en mer enhetlig tillämpning. Vad gäller personuppgifter vilka överförs till tredje land eller en internationell organisation, kräver förslaget att mottagaren ska uppnå en adekvat skyddsnivå för uppgifterna. Denna del ser ungefär ut som nuvarande reglering och kan förbättras avsevärt. De utomeuropeiska länder som EU-kommissionen ansett inneha en adekvat skyddsnivå är få. I de fall en adekvat skyddsnivå inte anses föreligga kommer samma situation uppkomma som idag, dvs. vid exempelvis överföring till USA blir det avgörande om mottagaren anslutit sig till de sk. Safe Harbor principerna. Möjligheten att använda någon av de tre standardavtalsklausuler vilka kommissionen godkänt kommer troligtvis finnas kvar och möjliggör att överföringen kan hålla den adekvata skyddsnivå vilken bedöms som tillräckligt enligt kommissionen. Verkligheten har dock visat att det inte är ovanligt att molntjänstjättar använder sig av sk. *Binding Corporate Rules*, eller användarvillkor, innehållande villkor vilka företaget själv tagit fram, främst med hänsyn till sitt eget hemlands lagstiftning. Google-exemplet visar att det är möjligt för en molntjänst att upprätta användarvillkor vilka uppenbarligen strider mot gällande EG-rätt utan att majoriteten av användare reagerar. Vad CNILs reaktion i form av 69 frågor till Google kommer leda till är i skrivande stund oklart, men utgången kommer av allt att döma att fastställa en rad sakfrågor vilka idag är oklara i fråga om personuppgiftsbehandling vid användande av molntjänster.

[166] Ilijason, a.a.

6.3 Överföring av personuppgifter till tredje land

Det är enligt PUL förbjudet att till tredje land föra över personuppgifter som är under behandling, eller ska behandlas där, om landet inte har en adekvat skyddsnivå för behandling av personuppgifter. Skyddsnivån bedöms av EU-kommissionen som tar hänsyn till samtliga omständigheter som har samband med överföringen. Det är idag totalt åtta länder, samt under vissa omständigheter Kanada och USA, vilka har bedömts inneha en adekvat skyddsnivå. Detta innebär att tillämpligheten för reglerna är begränsad. Det finns dock sätt att kringgå dessa regler; använda någon av de tre standardklausulerna som godkänts av EU-kommissionen eller på något annat sätt uppvisa tillräckliga garantier för skydd av den registrerades rättigheter, exempelvis genom sk. *Binding Corporate Rules*. De tre standardklausulerna är något som låter bra i teorin, men av datainspektionens granskningar kan utläsas att det i praktiken inte sällan är molntjänstleverantören som sätter upp sina egna användarvillkor utan hänsyn till varken standardklausuler eller nationell lag.

Dataskyddsförordningens regler vad gäller överföring till tredje land ser i stort ut på samma sätt som nuvarande regler i PUL. Detta är förvånande då personuppgifter överförs till tredje land i en allt större omfattning och snabbare takt vilket leder till att riskerna för integritetsintrång ökar och därmed även behovet för en harmoniserad reglering på området. Det kan dock vara så att EU-kommissionen tänker att den europeiska dataskyddsstyrelsen kommer utveckla arbetet med att bedöma vilka länder som innehar en adekvat skyddsnivå samt etablera användandet av de tre standardklausulerna bland företag utanför EU. Idén av en grupp bestående av representanter från vardera medlemsland vilken har större makt än den nuvarande Artikel 29-gruppen, är god. Gruppens inflytande kan göra att det bli möjligt med ett mer konsekvent beslutsfattande vilket kan ge tydliga riktlinjer. En förordning med krav på adekvat skyddsnivå väger tyngre mot molntjänstleverantörer i tredje land än nuvarande internationella lagstiftningar vilka bevisligen inte kan stå emot och påverka användarvillkor.[167]

6.4 Samtycke

Definitionen av samtycke spelar en avgörande roll vid behandling av personuppgifter i molntjänster då det bestämmer om en behandling är tillåten, med undantag för de fall då en behandling behövs av legitima skäl.

[167] Se de tre tillsynsbesluten från datainspektionen under avsnitt 4.1.1, 4.1.2 och 4.1.3.

PULs regler bygger på ett opt-out samtycke vilket innebär att det är tillräckligt med ett underförstått samtycke så länge behandlingen inte rör känsliga personuppgifter vilket kräver ett opt-in samtycke. Enligt dataskyddsförordningen är ett giltigt samtycke i de flesta situationer ett opt-in samtycke vilket innebär krav på en uttrycklig viljeyttring.

Det är tydligt att dataskyddsförordningen syftar till att stärka den personliga integriteten och ge registrerade mer makt och kontroll över sina uppgifter. Den höjda nivån på samtycke leder samtidigt till ökade administrativa belastningar för den personuppgiftsansvarige, genom den utökade dokumentationsskyldigheten, skyldigheten att genomföra konsekvensanalyser etc. Utformningen av samtycke är en av de mest omdebatterade delarna i förslaget och den slutgiltiga utformningen är ännu inte fastslagen enligt David Törngren vid justitiedepartementet.[168] Definitionen har redan ändrats från krav på opt-in samtycke till ett opt-out samtycke vid direkt marknadsföring, vilket innebär stora lättnader för företag vilka förlitar sig på att skicka ut meddelanden och reklam via e-post och via andra kommunikationsverktyg. En av de avgörande faktorerna till förändringar kan ha varit Tidningsutgivareföreningens (TUs) brev till EU-kommissionären Cecilia Malmström, enligt juristen Alexandra Lundvik vid TU.[169] I brevet skrevs det att ett opt-in samtycke vid alla former av direkt marknadsföring skulle innebära att ett företag i praktiken inte skulle kunna kontakta personer med vilka ett kundförhållande redan föreligger.[170]

Molntjänster vilka möjliggör e-handel är en av de parter vilka skulle komma att påverkas av ett strängare krav på samtycke. Svensk Handel har skrivit i sitt remissvar till förslaget att ett uttryckligt samtycke som ska lämnas oavsett personuppgifternas karaktär skulle innebära större aktiv handling för den registrerade och att detta i sin tur skulle minska förtroendet för e-handel. Ett ytterligare steg i processen i form av ”pop-up rutor” för köparen skulle innebära ett rent slentrianmässigt godkännande och en känsla av att bli överinformerad, vilket därmed inte skulle innebära någon höjning av säkerheten för den personliga integriteten, enligt Svensk Handel.[171] Det kan sammanfattas att dataskyddsdirektivet ställer ännu högre krav på vad ett samtycke innebär än PUL vilket innebär komplikation och större administrativa kostnader för molntjänstleverantörer samtidigt som det höjer integritetsskyddet för den registrerade.

---

[168] Intervju med David Törngren vid justitiedepartementet, 2012-04-27, kl. 10.00.
[169] Intervju med juristen Alexandra Lundvik vid Sveriges Tidningsutgivareföreningen (TU), 2012-06-19, kl. 11.00.
[170] Sveriges Tidningsutgivareföreningen (TU) brev till Cecilia Malmström, 2012-01-17, http://www.tu.se/images/stories/Document/TU_tycker/Remissvar/2012/PM2Dataskyddsforordning.pdf (2012-06-19, kl. 11.00).
[171] Svensk Handels remissyttrande, *Kommissionens förslag till dataskyddsförordning (KOM 2012) 11 slutlig).*

6.5 Molntjänsters användarvillkor

Betydelsen av användarvillkor är uppenbarligen stor, då det direkt påverkar användarens rättigheter och skyldigheter. Föreliggandet av användarvillkor vilka inte överensstämmer med dataskyddsdirektivet är nästintill bevisat genom CNILs kritik till Google. Som beskrivits ovan riskerar situationen att utvecklas till att det är upp till varje medlemsland att få Google att följa sin lagstiftning. En dialog kommer föras i första hand, och i andra hand kommer troligtvis sanktioner användas. Ett införande av förslagets hårdare sanktioner samt mer synkroniserad tillsynsorganisation skulle troligen skrämma förehavanden liknande Googles betydligt mer än dagens lagstiftning. Det finns idag ingen standardiserad utformning av användarvillkor för molntjänster. Förhoppningsvis är detta något den framtida dataskyddsstyrelsen enligt förslaget kan komma att ta fram. Eftersom betydelsen av utformningen av användarvillkor är så betydande för behandlingen av personuppgifterna och därmed skyddet för den registrerade tycks detta vara något dataskyddsstyrelsen torde prioritera.

6.6 Den personuppgiftsansvariges roll

Ansvarsområdet i PUL för den personuppgiftsansvarige är brett och i de fall en molntjänst lagrar eller behandlar data som innehåller personuppgifter ligger det på den personuppgiftsansvarige att PULs regler efterföljs, trots att tjänsten tillhandahålls av en molntjänstleverantör. PUL kräver att lämpliga tekniska och organisatoriska åtgärder åtas av den personuppgiftsansvarige och att denne ser till att molntjänstleverantören vidtar lämpliga skyddsåtgärder och att de kontrolleras genom ett avtal. I praktiken kan dessa krav vara svåra att genomföra då en molntjänstleverantör inte sällan är ovillig att samarbeta.[172]

Datainspektionen har hävdat i sina tre tillsynsbeslut att PUL inte är anpassat till den tekniska komplexitet som molntjänster innebär. I de tre besluten framkom att molntjänstleverantörerna styrde över användarvillkoren för behandlingen av personuppgifterna.[173] Bristerna vilka bedömdes föreligga vid användandet av molntjänster vid personuppgiftsbehandling, var att användaravtalen inte klargjorde att svensk lag gällde, avtalen reglerade inte att personuppgifter enbart får användas för förutbestämda ändamål, oklarhet om underleverantörers insyn och roll i behandlingen, oklarhet om vad som händer med personuppgifterna efter avtalet slutar gälla och oklarhet om kundens möjlighet att kontrollera att leverantören lever upp till

[172] Ahlsten, Fredrik & Bergenlind, Egil, *PUL ett hinder för molntjänster?* Dataföreningen.
[173] Se de tre tillsynsbesluten från datainspektionen under avsnitt 4.1.1, 4.1.2 och 4.1.3.

avtalsvillkoren.

De tre prövningarna visar att organisationer vilka använder sig av molntjänster bär ansvaret för personuppgiftsbehandlingen, trots att de hade tämligen små möjligheter att upprätta avtal i överensstämmelse med PUL eller granska molntjänstleverantörens säkerhetsnivå. Det kan konstateras att det enda praktiskt genomförbara och lagliga alternativet för de tre användarna var att avsluta användandet av respektive molntjänst. Reglerna enligt PUL innebär med andra ord att de tre väletablerade molntjänstleverantörerna, Dropbox, Windows Azure och Google Ireland Ltd inte kan användas på ett lagligt sätt vid behandling av personuppgifter i Sverige. Dessa tre, samt otaliga andra molntjänster, ställer upp användarvillkor utan anpassning efter i vilket land tjänsterna används i eller i vilket land personuppgifterna behandlas.

Vid nyttjande av molntjänster är det ofta en slags problematik som uppkommer; att ingen blir personuppgiftsbiträde vilket leder till ett icke hanterbart ansvar för den personuppgiftsansvarige. I PUL § 30 föreligger nämligen krav på ett personuppgiftsbiträdesavtal vilket leder till att molntjänstleverantören tar på sig detta ansvar. Emellertid ser verkligheten ut på ett sätt att molntjänstleverantörer inte alltid är villiga att skriva under ett sådant avtal. Detta gör att ansvaret för användaren av molntjänsten blir övermäktigt då ansvaret bland annat innebär att kontrollera att ett icke existerande personuppgiftsbiträde skyddar information.[174] Denna typ av situation visar att PUL och även dataskyddsförordningen utgår ifrån strikt åtskilda kategorier av aktörer (personuppgiftsansvarig, personuppgiftsbiträde m.fl.) vilket inte är lämpar sig till dynamiska och geografiskt oberoende molntjänster.

Det kan sammanfattas att ansvarsområdet för den personuppgiftsansvarige är stort i PUL och ännu större enligt dataskyddsförordningen. Förslaget tycks inte ta hänsyn till den obalans som föreligger idag till följd av att placera ansvaret på användaren av en molntjänst. Problemet grundar sig främst på att de kategorier av aktörer som både nuvarande lagstiftning samt förslaget bygger på inte är anpassningsbara efter molntjänstanvändande.

6.7 Missbruksregeln och hanteringsmodellen

Vid införandet av PUL gjorde riksdagen en uppdelning mellan de strängare hanteringsreglerna för strukturerad behandling i registerform, och missbruksregeln för ostrukturerad behandling. Dataskyddsförordningen tar

[174] Ilijason, a.a.

bort denna uppdelning och är istället utformad enligt en hanteringsmodell vilken innebär att själva hanteringen av personuppgifter regleras från det att uppgifterna samlas in till dess att de utplånas. En hanteringsmodell kan hindra en kränkning av den personliga integriteten redan innan det sker, istället för att straffa en handling vilken redan skett. Flera remissinstanser har motsatt sig förslagets borttagande av missbruksregeln. En av de remissinstanserna är Sveriges Kommuner och Landssting vilka har skrivit i sitt remissvar att ett borttagande skulle innebära en tillämpning av de stränga och mer komplicerade hanteringsreglerna vid harmlös personuppgiftsbehandling, såsom publicering i löpande text på webbplatser.[175] Rättsläget skulle likna det som var gällande i Sverige innan missbruksregeln infördes den 1 januari 2007. Vid denna tid förelåg stor osäkerhet över vilka möjligheter som fanns för att publicera texter och bilder på Internet och webbplatser.[176] Förslaget kompenserar dock borttagandet av missbruksregeln med att medlemsstaterna får rätt att skapa undantag för behandling som sker uteslutande för journalistiska, konstnärliga och litterära ändamål, vilket motsvarar de undantag som föreligger i PUL till skydd för tryck- och yttrandefriheten. Som nämnts ovan är det dock oklart i vilken mån detta undantag kommer att kunna tillämpas. Vad som går att konstatera är att en lagstiftning i form av en förordning, minskar automatiskt medlemsstaternas bestämmanderätt.

6.8 Tillsyn vid överträdelse av reglerna

Tillsynen i PUL jämfört med dataskyddsförordningen skiljer sig åt på flera plan. Datainspektionen är Sveriges nationella tillsynsmyndighet för behandling av personuppgifter och har som syfte att bidra till att inga intrång i enskildas personliga integritet förekommer.[177] EU-kommissionen föreslår i förordningen att en europeisk dataskyddsstyrelse, bestående av representanter från de nationella dataskyddsmyndigheterna, ska införas. Denna grupp kommer ersätta den nuvarande arbetsgruppen för uppgiftsskydd, den s.k. Artikel 29-gruppen, som tillskapades enligt dataskyddsdirektivet. Den europeiska dataskyddsstyrelsen kommer inneha en mer central och inflytelserik roll över medlemsstaterna än Artikel 29-gruppen. Det kommer därmed föreligga ett mer konsekvent tillämpande av reglerna i EU än idag, vilket är positivt för ett område som molntjänster som verkar gränsöverskridande.

Vidare skiljer sig förslaget åt på så sätt att de nationella

---

[175] Sveriges Kommuner och Landssting, *Kommissionens förslag till dataskyddsförordning (KOM (2012) 11 slutlig)*.
[176] Ibid.
[177] Enligt Schengenkonventionen, konventionen om EU:s tullinformationssystem samt rådsbeslutet om inrättande av Europeiska polisbyrån (Europol).

tillsynsmyndigheterna är skyldiga att besluta om administrativa sanktionsavgifter vid vissa överträdelser av förordningen. Beloppen som ska dömas ut är betydligt högre än de som någonsin kan komma på tal i Sverige idag.[178] Som tidigare angetts, behöver en del av ansvaret lyftas från användaren av en molntjänst till molntjänstleverantören. Sanktioner som kan hamna på molntjänstleverantören kan vara en lösning på problemet med hänsynslösa användarvillkor då det leder till att leverantören bär ett större ansvar med risk för påföljd. I annat fall kan dessa höga sanktioner ha förödande effekter på molntjänstanvändare.

Efter att ha granskat datainspektionens beslut, kan det konstateras att molntjänsterna Google, Dropbox och Windows Azure agerar utan hänsyn till PULs regler. Utan att göra en grundlig undersökning kan det antas att många andra molntjänster agerar på samma sätt. En förordning, med dataskyddsstyrelsen i spetsen med hjälp av nationella dataskyddsmyndigheter, vilka kan besluta om administrativa sanktionsavgifter även till molntjänstleverantörer, kan komma att påverka utformningen av användarvillkor. Därmed kan en säkrare behandling av personuppgifter i molntjänster bli verklighet.

[178] Se under avsnitt 3.6.

7. Avslutande reflektioner

Som flera gånger påpekats medför den indirekta harmoniseringen av det gällande dataskyddsdirektivet ett antal komplikationer vid tillämpning av reglerna i kombination med molntjänstanvändande. Det territoriella tillämpningsområdet i PUL gör att ett mörkertal av aktörer undviker lagen med hjälp av den lucka som föreligger i reglerna om tillämplig lag. Förekommandet av personuppgifter vilka överförs till ett tredje land utan en adekvat skyddsnivå eller annan garanti tycks förekomma ideligen trots att en sådan överföring är förbjuden. Förordningsförslaget tycks inte göra något konkret åt detta problem förutom införandet av en europeisk dataskyddsstyrelse. Förhoppningsvis kan styrelsen, med förordningsreglerna som grund och med medlemsländerna i ryggen, sätta press på molntjänstleverantörer att upprätta användarvillkor vilka går i linje med en harmoniserad förordning.

I relation till uppmärksamheten kring Googles användarvillkor, kan det förutspås att liknande situationer kommer uppstå med andra molntjänstleverantörer om inte tydligare regler för användarvillkor upprättas. Det är inte molntjänster i sig som står i strid med ansvaret i PUL eller förslaget, problemet ligger i att användarvillkoren är otydliga. Vad som behövs är en lagstiftning som ställer krav på tydliga användarvillkor med obligatoriska punkter vilka är essentiella för ett säkert molntjänstanvändande. Vidare ställer förordningsförslagets hanteringsmodell en större säkerhetsnivå då personuppgiftsbehandling kan granskas från första stund och missbruk och intrång kan förhindras redan innan det skett.

Den personuppgiftsansvariges ansvarsområde är inte praktiskt genomförbart i förslaget eller i PUL vid behandling av personuppgifter i molntjänster. Det visar datainspektionens granskningar. Ett gemensamt problem för de båda regleringarna är kategoriseringarna av aktörer vilka inte fungerar i relation till molntjänstanvändande. En uppdelning av ansvaret mellan användaren av molntjänsten samt leverantören skulle möjliggöra att den sistnämndas ovilja att samarbeta minskade, särskilt i det fall de administrativa sanktionsavgifterna skulle komma att falla på denne.

Tillsynen är enligt förordningsförslaget mer harmoniserat och utformat på ett sätt som kräver samarbete mellan medlemsländerna. Den europeiska dataskyddsstyrelsen kommer agera och bestå av representanter från EU med mer makt än den nuvarande Artikel 29-gruppen. En arbetsgrupp som denna vilken kontinuerligt har som syfte att arbeta för utvecklingen är oerhört relevant för molntjänster vilka hela tiden förändras. De administrativa sanktionsavgifter vilka de nationella tillsynsmyndigheterna ges möjlighet att besluta om är ytterligare något som är positivt för skyddet av personuppgifter i molntjänster då det möjliggör en harmoniserad

tillsynsorganisation i hela EU. Detta förutsätter dock att den personuppgiftsansvariges ansvarsområde förs över till molntjänstleverantören i de delar som idag är praktiskt omöjliga att ansvara över.

I förhållande till skydd för personuppgifter vilka behandlas i molntjänster väger skälen över för en förordning före ett direktiv. I de svenska remissvaren, regeringens yttrande till EU-kommissionen och KUs utlåtande verkar dock en viss motvilja mot en harmoniserad lagstiftning i form av en förordning föreligga. Oavsett om de nya reglerna får formen av ett direktiv eller förordning kan det inte annat än konstateras att det kommer vara en förbättring mot dagens reglering. PUL och dataskyddsdirektivet togs fram med utgångspunkt i en annan teknisk miljö än den rådande. Vid tiden för utformningen av direktivet var fristående personregister den mest använda metoden vid hantering av personuppgifter. Numera används molntjänster för vardaglig ostrukturerad hantering av personuppgifter. Det kan konstateras att en moderniserad lagstiftning är behövlig då nya utmaningar har uppkommit till följd av en snabb teknisk utveckling. Insamling och utlämnande av personuppgifter har ökat i omfattning och en enhetlig grund som de nationella tillsynsmyndigheterna kan verka efter skulle leda till mer likartade beslut. Framtidens lagstiftning för skydd av personuppgifter behöver vara flexibel och användarcentrerad. Flexibel för att den ska kunna stödja mängden av identitetsmekanismer som existerar och fortfarande uppkommer inom molntjänstvärlden. Användarcentrerad för att slutanvändarna är kärnan av identitetshanteringen. Får användare utöva effektiv kontroll över deras personuppgiftsbehandling kan de höga krav som föreligger idag och i förslaget bli rationella. Detta bemötande till digital identitet skulle släppa loss molntjänsters fulla potential, och möjliggöra för användare att utöva kontroll samt ställa krav på molntjänstleverantörer.

Käll- och litteraturförteckning

Offentligt tryck

Sverige

SFS 2011:127 Lag om ändring i lagen (2002:546) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten

SFS 2011:109 Regeringsformen

SFS 2009:400 Offentlighets- och sekretesslag

SFS 2002:546 Lag om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten

SFS 1998:204 Personuppgiftslag

SFS 1973:289 Datalagen

SFS 2010:1458 Skadeståndslagen

SFS 2002:546 Lagen om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten

SOU 1999:105 Skatt – Tull – Exekution – Normer för behandling av personuppgifter

Prop. 2010/11:42 Borttagande av kravet på samtycke för behandlingen av vissa personuppgifter i den arbetsmarknadspolitiska verksamheten

Prop. 2005/06:173 Översyn av personuppgiftslagen

Prop. 2001/02:144 Lag om behandling av behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten

Prop. 2000/01:33 Behandling av personuppgifter inom skatt, tull och exekution

Prop. 1997/98:44 Personuppgiftslag

Ds 2010:33 Borttagande av samtyckeskravet för behandling av känsliga och ömtåliga personuppgifter i den arbetsmarknadspolitiska verksamheten

Ds 2001:67 Behandling av personuppgifter i den arbetspolitiska verksamheten

Ds 2001:27 EG-direktivet om personuppgifter - en offentlig utvärdering

Bet. 1997/98:KU18 Personuppgiftslagen

Riksdagsskrivelse 2011/12:178

Konstitutionsutskottet, *Utlåtande 2011/12:KU25 EU-förslag om allmän uppgiftsskyddsförordning*

Justitiedepartementet, *Faktapromemoria 2011/12:FPM117 Allmän dataskyddsförordning*

Datainspektionen, *Molntjänster och Personuppgiftslagen*, 2011

Datainspektionen, *Personuppgiftsansvar*, 2010

Datainspektionens rapport, *Personuppgifter i genforskning – uppföljning av förhandskontroller*, 2002:4

EU

Article 29 data protection working group, *Opinion 05/2012 on Cloud Computing*.

Artikel 29-gruppen, *Yttrande 15/2011 om definitionen av begreppet ”samtycke”*, 01197/11/SV WP187

Europeiska kommissionen, *beslut av den 27 december 2004 om ändring av beslut 2001/497/EG om standardavtalsklausuler för överföring av personuppgifter till tredje land*

Europeiska kommissionen, *beslut av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbor Privacy Principles) i kombination med frågor och svar som Förenta staterna handelsministerium utfärdat EGT L 215*

Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och det fria flödet av sådana uppgifter

Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter

Lissabonfördraget om ändring av fördraget om Europeiska unionen och fördraget om upprättandet av Europeiska gemenskapen

Lissabonfördraget, Protokoll om tillämpning av subsidiaritets- och proportionalitetsprinciperna

Schengenkonventionen, konventionen om EU:s tullinformationssystem samt rådsbeslutet om inrättande av Europeiska polisbyrån (Europol)

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard of the processing of personal data and on the free movement of such data, European Commission, Brussels, 25.1.2012. COM(2012) 11 final

USA

National Institute of Standards and Technology, *The NIST Definition of Cloud Computing*

Litteratur

Böcker och monografier

Blomberg, Kristina, *Värt att veta om Personuppgiftslagen*, Studentlitteratur, Lund, 2012.

Christner, Anders & Edvardsson, Tobias. *Cloud Computing: en handledning och kommentar till IT & Telekomföretagens standardavtal Cloud Computing version 2010*, IT & Telekomföretagen, Stockholm, 2011.

Lindberg, Agne & Westman, Daniel, *Praktisk IT-rätt*, Nordstedts Juridik AB, Stockholm, 3e uppl., 2001.

Menken, Ivanka, *An introduction to Cloud Computing*, Emereo publishing. Brisbane, 2011.

Rejdnell, Jan, *Den personliga integriteten behöver stärkas*, Newsmill, http://www.newsmill.se/artikel/2012/03/29/nu-beh-vs-konkreta-f-rslag-att-st-rka-personliga-integriteten (2012-05-28, kl. 15.00).

Öman, Sören & Lindblom, Hans-Olof, *Personuppgiftslagen, En kommentar*, 4e uppl., Nordstedts Juridik AB, Stockholm, 2011.

Artiklar

Ahlsten, Fredrik & Bergenlind, Egil, *PUL ett hinder för molntjänster?*

Dataföreningen, hämtad från Tidnings- och tidsskriftsbiblioteket, Stockholm (2012-05-28, kl. 15.30).

Björklund, Karl-Fredrik & Johnssén, Filip, *Nya förenklade regler i personuppgiftslagen*, Advokaten, nr 7, 2007, Årgång 73, http://www.advokatsamfundet.se/Advokaten/Tidningsnummer/2007/Nr-7-2007-Argang-73/Nya-forenklade-regler-i-personuppgiftslagen/ (2012-06-19, kl. 15.00).

Carr G., Nicholas, *The End of Corporate Computing*, MIT Sloan Management Review vol. 46, nr 3, 2005, s. 67-73.

Falk, Johan, *Cloud Computing*, Forskning & Framsteg, nr 6/2009, s. 12-17.

Gellman, Robert, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, The World Privacy Forum, 2009-02-23, http://www.worldprivacyforum.org/cloudprivacy.html (2012-06-19, kl. 14.30).

Haglund, Fredrik, *Europeiska dataskyddsmyndigheter har bett Google svara på en rad frågor om företagets nya användarvillkor, Europaportalen*, http://www.europaportalen.se/2012/03/europeiska-datamyndigheter-ifragasatter-google (2012-05-24, kl.15.30).

Hellström, Roger, *På molnfronten intet nytt? Vissa rättsliga aspekter på molntjänster*, Ny Juridik 2:11, Thomson Reuters Professional AB, 2011.

Ilijason, Roberg, *PUL-stormen hotar molnet*, Tech World, vol/nr: 2012: 1-2, 4.

Molin, Åsa, *Att våga lita på webbmoln*, Dagen, 2012-01-04, hämtad från Tidnings- och tidsskriftsbiblioteket, Stockholm, (2012-01-04), s. 12-13.

Rolfer, Andreas, *Knepigt få Google att ändra sig*, Dagens Nyheter, http://www.dn.se/ekonomi/knepigt-fa-google-att-andra-sig?rm=print (2012-05-24, kl.15.00).

Sjögren, Per-Anders, *Rätt att radera uppgifter om privatlivet från Internet*, Riksdag & Parlament, 2012-01-30, hämtad från Tidnings- och tidsskriftsbiblioteket, Stockholm, (2012-04-13, kl.13.30), s. 12.

Svensson, Daniel, *Möjligheter och risker i Molnet*, Skydd & Säkerhet, Säkerhetsbranschens månadstidning, Nr 3:2011, s. 42-43.

Yousef, L., Butrico, M. & Da Silva, D., *Toward a Unified Ontology of*

Cloud Computing,
http://www.cs.ucsb.edu/~lyouseff/CCOntology/CloudOntology.pdf
(2012-05-18, kl. 16.00).

- *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses*, European Commission, 2012-01-25,
http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46
(2012-05-24, kl. 10.30).

- *Final version of NIST Cloud Computing Definition Published*, NIST Tech Beat, 2011-10-25,
http://www.nist.gov/itl/csd/cloud-102511.cfm
(2012-03-29, kl.10.30).

- *The Privacy Implications of Cloud Computing*, Privacy Rights Clearinghouse,
http://www.privacyrights.org/ar/cloud-computing.htm
(2012-05-14, kl. 14.00).

- *Risker med otydliga avtal för molntjänster*, Mitt i Juridiken, 2011-11-30, hämtad från Tidnings- och tidsskriftsbiblioteket, Stockholm, (2012-04-13, kl. 14.00).

Övrigt

City Clouds affärsidé,
http://www.citycloud.se/service-provider-2/
(2012-05-18, kl. 14.00).

City Cloud – en molntjänst från City Network,
http://www.citycloud.se/
(2012-04-04, kl. 16.00).

CNILs 69 frågor till Google,
http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/questionnaire_to_Google-2012-03-16.pdf (2012-06-19).

Dropbox – en molntjänst,
https://www.dropbox.com/,
(2012-04-25, kl. 16.00).

Europeiska kommissionens standardklausuler,
www.ec.europa.eu
(2012-06-01, kl. 14.00).

Google App Engine,

https://developers.google.com/appengine/
(2012-04-25, kl. 17.30).

Google Drive – en molntjänst från Google,
https://drive.google.com/start#home,
(2012-04-25, kl. 16.00).

Googles användarvillkor,
http://www.google.com/policies/terms/
(2012-05-24, kl.15.30).

Googles policyer och principer,
http://www.google.com/intl/sv/policies/
(2012-05-19, kl. 14.00).

iCloud – en molntjänst från Apple,
https://www.icloud.com/,
(2012-04-25, kl. 16.00).

Interparliamentary Exchange, *Document COM/2012/0011*,
http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20120011.do
(2012-05-14, kl.14.00).

Microsoft Office,
http://www.microsoft.com/sv-se/office365/online-software.aspx
(2012-05-16, kl. 13.00).

Svensk Handels remissyttrande, *Kommissionens förslag till dataskyddsförordning (KOM 2012) 11 slutlig)*, 2012-03-09.

Sveriges Kommuner och Landssting, *Kommissionens förslag till dataskyddsförordning (KOM (2012) 11 slutlig)*, 2012-03-09.

Sveriges Tidningsutgivareföreningen (TU) brev till Cecilia Malmström, 2012-01-17,
http://www.tu.se/images/stories/Document/TU_tycker/Remissvar/2012/PM2Dataskyddsforordning.pdf
(2012-06-19, kl. 11.00).

SVT on demand i digital-tv-box,
http://www.copyswede.se/2012/01/svt-on-demand-i-digital-tv-box/
(2012-04-25, kl. 14.30).

Intervjuer

Intervju med juristen David Törngren vid justitiedepartementet, 2012-04-27, kl. 10.00.

Intervju med juristen Alexandra Lundvik vid Sveriges Tidningsutgivareföreningen (TU), 2012-06-19, kl. 11.00.

Intervju med juristen Anna Hörnlund vid datainspektionen, 2012-06-07, kl. 17.00.

Rättsfallsförteckning

EG-domstolen

EG-domstolens avgörande den 6 november 2003 i mål C-101/01.

Sverige

Högsta Domstolens dom den 26 maj 2005, NJA 2005 s. 361.

Göta Hovrätts dom den 7 april 2004 i mål nr B-747/00.

Helsingborgs tingsrätts dom den 31 januari 2001 i mål nr B 3915-00.

Justitiekanslerns beslut den 28 mars 2003, diarienummer 73-02-42.

Datainspektionen

Datainspektionens beslut i ärendet: Tillsyn enligt personuppgiftslagen (1998:204) – Enköpings kommunstyrelses användning av molntjänsten Dropbox, 2011-09-28, diarienummer: 256-2011.

Datainspektionens beslut i ärendet: Tillsyn enligt personuppgiftslagen (1998:204) – Brevo AB, 2011-09-28. diarienummer: 574-2011.

Datainspektionens beslut i ärendet: Tillsyn enligt personuppgiftslagen (1998:204) – Salems kommunstyrelse, 2011-09-28, diarienummer: 263-2011.

Datainspektionens beslut i ärendet: Tillsyn enligt personuppgiftslagen (1998:204) mot IOGT-NTO – behandling av uppgifter i medlemsregister. 2008-08-06, diarienummer 217-2008.

Datainspektionens beslut i ärendet: Tillsyn enligt personuppgiftslagen (1998:204) – hantering av personnummer i samband med prisförfrågan. 2007-10-08, diarienummer 246-2007.

Datainspektionens beslut i ärendet: Beslut efter tillsyn enligt personuppgiftslagen (1998:204), 2006-12-12, diarienummer 1082-2006.

Bilaga A

National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-145

The NIST Definition of Cloud Computing

Recommendations of the National Institute of Standards and Technology

Peter Mel
Timothy Grance

NIST Special Publication 800-145 **The NIST Definition of Cloud Computing**

Peter Mell
Timothy Grance

C O M P U T E R SEC U R I TY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September 2011

U.S. Department of Commerce

Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology

Patrick D. Gallagher, Under Secretary for Standards and Technology and Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-145

7 pages (September 2011)

Acknowledgements

The authors Peter Mell and Timothy Grance of the National Institute of Standards and Technology (NIST) would like to thank the many experts in industry and government who contributed their thoughts to the creation and review of this definition. We especially acknowledge Murugiah Souppaya and Lee Badger, also of NIST, and Wayne Jansen of Booz Allen Hamilton, whose advice and technical insight assisted this effort.

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets; but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

1.2 Purpose and Scope

Cloud computing is an evolving paradigm. The NIST definition characterizes important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. The service and deployment models defined form a simple taxonomy that is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation.

1.3 Audience

The intended audience of this document is system planners, program managers, technologists, and others adopting cloud computing as consumers or providers of cloud services.

2. The NIST Definition of Cloud Computing

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics**,** three service models, and four deployment models.

Essential Characteristics:

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability[1] at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service Models:

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure[2]. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming

[1] Typically this is done on a pay-per-use or charge-per-use basis.

[2] A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

languages, libraries, services, and tools supported by the provider.[3] The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

[3] This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.

Bilaga B

ARTICLE 29 DATA PROTECTION WORKING PARTY

01037/12/EN
WP 196

Opinion 05/2012 on Cloud Computing

Adopted July 1st 2012

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

Executive Summary

In this Opinion the Article 29 Working Party analyses all relevant issues for cloud computing service providers operating in the European Economic Area (EEA) and their clients specifying all applicable principles from the EU Data Protection Directive (95/46/EC) and the e-privacy Directive 2002/58/EC (as revised by 2009/136/EC) where relevant.

Despite the acknowledged benefits of cloud computing in both economic and societal terms, this Opinion outlines how the wide scale deployment of cloud computing services can trigger a number of data protection risks, mainly a lack of control over personal data as well as insufficient information with regard to how, where and by whom the data is being processed/sub-processed. These risks need to be carefully assessed by public bodies and private enterprises when they are considering engaging the services of a cloud provider. This Opinion examines issues associated with the sharing of resources with other parties, the lack of transparency of an outsourcing chain consisting of multiple processors and subcontractors, the unavailability of a common global data portability framework and uncertainty with regard to the admissibility of the transfer of personal data to cloud providers established outside of the EEA. Similarly, a lack of transparency in terms of the information a controller is able to provide to a data subject on how their personal data is processed is highlighted in the opinion as matter of serious concern. Data subjects must[1] be informed who processes their data for what purposes and to be able to exercise the rights afforded to them in this respect.

A key conclusion of this Opinion is that businesses and administrations wishing to use cloud computing should conduct, as a first step, a comprehensive and thorough risk analysis. All cloud providers offering services in the EEA should provide the cloud client with all the information necessary to rightly assess the pros and cons of adopting such a service. Security, transparency and legal certainty for the clients should be key drivers behind the offer of cloud computing services.

In terms of the recommendations contained in this Opinion, a cloud client's responsibilities as a controller is highlighted and it is thus recommended that the client should select a cloud provider that guarantees compliance with EU data protection legislation. Appropriate contractual safeguards are addressed in the opinion with the requirement that any contract between the cloud client and cloud provider should afford sufficient guarantees in terms of technical and organizational measures. Also of significance is the recommendation that the cloud client should verify whether the cloud provider can guarantee the lawfulness of any cross-border international data transfers.

Like any evolutionary process, the rise of cloud computing as a global technological paradigm represents a challenge. This Opinion, as it stands, can be deemed to be an important step in defining the tasks to be assumed in this regard by the data protection community in the upcoming years.

[1] The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in Request for Comments 2119. The document is available at http://www.ietf.org/rfc/rfc2119.txt. However, for readability, these words do not appear in all uppercase letters in this specification.

Table of Contents

1. Introduction

For some, cloud computing is one of the biggest technological revolutions to emerge in recent times. For others, it is just the natural evolution of a set of technologies aimed to achieve the long awaited dream of utility computing. In any case, large numbers of stakeholders have put cloud computing to the fore in the development of their technological strategies.

Cloud computing consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space. Cloud computing can generate important economic benefits, because on-demand resources can be configured, expanded and accessed on the Internet quite easily. Next to economic benefits, cloud computing may also bring security benefits; enterprises, especially small-to-medium sized ones, may acquire, at a marginal cost, top-class technologies, which would otherwise be out of their budget range.

There is a wide gamut of services offered by cloud providers ranging from virtual processing systems (which replace and/or work alongside conventional servers under the direct control of the controller) to services supporting application development and advanced hosting, up to web-based software solutions that can replace applications conventionally installed on the personal computers of end-users. This includes text processing applications, agendas and calendars, filing systems for online document storage and outsourced email solutions. Some of the most commonly used definitions for these different types of services are contained in the Annex to this Opinion.

In this Opinion the Article 29 Working Party (hereinafter: WP 29) analyses the applicable law and obligations for controllers in the European Economic Area (hereinafter: EEA) and for cloud service providers with clients in the EEA. This opinion focuses on the situation, where the relationship is assumed to be a controller-processor relationship, with the customer qualifying as controller and the cloud provider qualifying as processor. In cases where the cloud provider acts as a controller as well, they have to meet additional requirements. As a consequence, a precondition for relying on cloud computing arrangements is for the controller to perform an adequate risk assessment exercise, including the locations of the servers where the data are processed and the consideration of risks and benefits from a data protection perspective, pursuant to the criteria outlined in the paragraphs below.

This Opinion specifies the applicable principles for both controllers and processors from the general data protection directive (95/46/EC), such as purpose specification and limitation, erasure of data and technical and organizational measures. The opinion provides guidance on the security-requirements, both as a structural and a procedural safeguard. Special emphasis is laid on the contractual arrangements that should regulate the relationship between a controller and a processor in this connection. The classic goals of data security are availability, integrity and confidentiality. However, data protection is not limited to data security and therefore these goals are complemented with the specific data protection goals of transparency, isolation, intervenability and portability to substantiate the individual's right to data protection as enshrined in Article 8 of the EU Charter of Fundamental rights.

With regard to transfers of personal data outside of the EEA, instruments such as the standard contractual clauses adopted by the European Commission, adequacy-findings and a possible future processor-BCR are analysed, as well as data protection risks arising from international law enforcement requests.

This Opinion concludes with recommendations for cloud clients as controllers, cloud providers as processors and for the European Commission with regard to future changes in the European data protection framework.

The Berlin International Working Group on Data Protection in Telecommunications adopted the *Sopot Memorandum*[2] in April 2012. This memorandum examines privacy and data protection issues in cloud computing and emphasizes that cloud computing must not lead to a lowering of data protection standards as compared to conventional data processing.

2. Data protection risks of cloud computing

As this Opinion focuses on personal data processing operations deploying cloud computing services, only the specific risks related to this context are considered.[3] The majority of these risks fall within two broad categories namely lack of control over the data, and insufficient information regarding the processing operation itself (absence of transparency). Specific cloud computing risks considered in this opinion include:

Lack of control

By committing personal data to the systems managed by a cloud provider, cloud clients may no longer be in exclusive control of this data and cannot deploy the technical and organisational measures necessary to ensure the availability, integrity, confidentiality, transparency, isolation[4], intervenability and portability of the data. This lack of control may manifest itself in the following manner:

- Lack of availability due to lack of interoperability (vendor lock-in): If the cloud provider relies on proprietary technology it may prove difficult for a cloud client to shift data and documents between different cloud-based systems (data portability) or to exchange information with entities that use cloud services managed by different providers (interoperability).
- Lack of integrity caused by the sharing of resources: A cloud is made up of shared systems and infrastructures. Cloud providers process personal data emanating from a wide range of sources in terms of data subjects and organisations and it is a possibility that conflicting interests and/or different objectives might arise.
- Lack of confidentiality in terms of law enforcement requests made directly to a cloud provider: personal data being processed in the cloud may be subject to law enforcement requests from law enforcement agencies of the EU Member States and of third countries. There is a risk that personal data could be disclosed to (foreign) law enforcement agencies without a valid EU legal basis and thus a breach of EU data protection law would occur.
- Lack of intervenability due to the complexity and dynamics of the outsourcing chain: The cloud service offered by one provider might be produced by combining services from a range of other providers, which may be dynamically added or removed during the duration of the client's contract.

---

2 http://datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf

3 In addition to the risks related to personal data processed "in the cloud" explicitly mentioned in this opinion, all risks related to the outsourcing of the processing of personal data must also be taken into account.

4 In Germany the broader concept of "unlinkability" has been introduced. Cf. footnote 24 below.

- Lack of intervenability (data subjects' rights): A cloud provider may not provide the necessary measures and tools to assist the controller to manage the data in terms of, e.g., access, deletion or correction of data.
- Lack of isolation: A cloud provider may use its physical control over data from different clients to link personal data. If administrators are facilitated with sufficiently privileged access rights (high-risk roles), they could link information from different clients.

Lack of information on processing (transparency)

Insufficient information about a cloud service's processing operations poses a risk to controllers as well as to data subjects because they might not be aware of potential threats and risks and thus cannot take measures they deem appropriate.

Some potential threats may arise from the controller not knowing that

- Chain processing is taking place involving multiple processors and subcontractors.
- Personal data are processed in different geographic locations within the EEA. This impacts directly on the law applicable to any data protection disputes which may arise between user and provider.
- Personal data is transferred to third countries outside the EEA. Third countries may not provide an adequate level of data protection and transfers may not be safeguarded by appropriate measures (e.g., standard contractual clauses or binding corporate rules) and thus may be illegal.

It is a requirement that data subjects whose personal data are processed in the cloud are informed as to the identity of the data controller and the purpose of the processing (an existing requirement for all controllers under Data Protection Directive 95/46/EC). Given the potential complexity of processing chains in a cloud computing environment, in order to guarantee fair processing in respect of the data subject (Article 10 of Directive 95/46/EC), controllers should also as a matter of good practice provide further information relating to the (sub-)processors providing the cloud services.

3. Legal framework

3.1 Data protection framework

The relevant legal framework is the Data Protection Directive 95/46/EC. This Directive applies in every case where personal data are being processed as a result of the use of cloud computing services. The e-privacy Directive 2002/58/EC (as revised by 2009/136/EC) applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks (telecom operators) and thus is relevant if such services are provided by means of a cloud solution[5].

[5] Directive 2002/58/CE on e-privacy (as amended by Directive 2009/136/CE): Directive 2002/58/EC on privacy in telecommunications applies to providers of electronic communication services made available to the public, and requires them to ensure compliance with obligations relating to the secrecy of communications and personal data protection, as well as rights and obligations with regard to electronic communications networks and services. In cases where cloud computing providers act as providers of a publicly-available electronic communication service they will be subject to this regulation.

3.2 Applicable law

The criteria for establishing the applicability of legislation are contained in Article 4 of Directive 95/46/EC, which refers to the law applying to controllers[6] with one or more establishments within the EEA and also to the law applying to controllers who are outside the EEA but use equipment located within the EEA to process personal data. The Article 29 Working Party has analyzed this issue in its Opinion 8/2010 on applicable law[7].

In the first case, the factor that triggers the application of EU law to the controller is the location of his or her establishment and the activities it carries out, according to Article 4.1.a) of the Directive, with the type of cloud service model being irrelevant. The applicable legislation is the law of the country in which the controller contracting the cloud computing services is established, rather than the place in which the cloud computing providers are located.

Should the controller be established in various Member States, processing the data as part of its activities in these countries, the applicable law shall be that of each of the Member States in which this processing occurs.

Article 4.1.c)[8] refers to how data protection legislation applies to controllers who are not established in the EEA but use automated or non-automated equipment located in the territory of the Member State, except where these are used only for purposes of transit. This means that if a cloud client is established outside the EEA, but commissions a cloud provider located in the EEA, then the provider exports the data protection legislation to the client.

3.3 Duties and responsibilities of different players

As previously indicated, cloud computing involves a range of different players. It is important to assess and clarify the role of each of these players in order to establish their specific obligations with regard to current data protection legislation.

It should be recalled that the WP29 pointed out in its opinion 1/2010 on the concepts of "controller" and "processor" that "*the first and foremost role of the concept of controller is to determine who shall be responsible for compliance with data protection rules, and how data subjects can exercise the rights in practice. In other words: to allocate responsibility.*" These two general criteria responsible for compliance and allocation of responsibility should be borne in mind by the parties involved throughout the analysis in question.

3.3.1 Cloud client and cloud provider

The cloud client determines the ultimate purpose of the processing and decides on the outsourcing of this processing and the delegation of all or part of the processing activities to an external organisation. The cloud client therefore acts as a data controller. The Directive defines a controller as "*the natural or legal person, public authority, agency or any other body that alone or jointly with others determines the purposes and means of the processing of*

---

6 The concept of the controller can be found in Article 2.h) of the Directive and was analysed by the Article 29 WG in its Opinion 1/2010 on the concepts of controllers and processors.

7 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf

8 Article 4(1)c states that the legislation of a Member State shall be applicable when "the controller is not established in Community territory and, for purposes of processing personal data, makes use of equipment, automated or otherwise, situated in the territory of said Member State, unless such equipment is used only for purposes of transit through the territory of the Community".

personal data". The cloud client, as controller, must accept responsibility for abiding by data protection legislation and is responsible and subject to all the legal duties that are addressed in Directive 95/46/EC. The cloud client may task the cloud provider with choosing the methods and the technical or organisational measures to be used to achieve the purposes of the controller.

The cloud provider is the entity that provides the cloud computing services in the various forms discussed above. When the cloud provider supplies the means and the platform, acting on behalf of the cloud client, the cloud provider is considered as a data processor i.e., according to Directive 95/46/EC "*the natural or legal person, public authority, agency or any other body that alone or jointly with others, processes personal data on behalf of the controller*".[9][10]

As stated in the Opinion 1/2010, some criteria[11] can be used for assessing controllership of the processing. As a matter of fact, there may be situations in which a provider of cloud services may be considered either as a joint controller or as a controller in their own right depending on concrete circumstances. For instance, this could be the case where the provider processes data for its own purposes.

It should be emphasized that even in complex data processing environments, where different controllers play a role in processing personal data, compliance with data protection rules and responsibilities for possible breach of these rules must be clearly allocated, in order to avoid that the protection of personal data is reduced or that a "negative conflict of competence" and gaps arise whereby some obligations or rights stemming from the Directive are not ensured by any of the parties.

In the current cloud computing scenario, clients of cloud computing services may not have room for manoeuvre in negotiating the contractual terms of use of the cloud services as standardised offers are a feature of many cloud computing services. Nevertheless, it is ultimately the client who decides on the allocation of part or the totality of processing operations to cloud services for specific purposes; the cloud provider's role will be that of a contractor vis-à-vis the client, which is the key point in this case. As stated in the Article 29 Working Party Opinion 1/2010[12] on the concepts of controller and processor, "*the imbalance in the contractual power of a small controller with respect to large service providers should not be considered as a justification for the controller to accept clauses and terms of contracts which are not in compliance with data protection law*". For this reason, the controller must choose a cloud provider that guarantees compliance with data protection legislation. Special emphasis must be placed on the features of the applicable contracts – these must include a set of standardised data protection safeguards including those outlined by the WP in paragraph 3.4.3 (Technical and Organisational Measures) and in paragraph 3.5 (cross-border data flows) – as well as on additional mechanisms that can prove suitable for facilitating due diligence and accountability (such as independent third-party audits and certifications of a provider's ~~services – see paragraph 4.2).~~

[9] This opinion focuses only on the regular controller – processor relationship.

[10] The cloud computing environment can also be used by natural persons (users) to carry out exclusively personal or domestic activities. In such a case, it is to be analysed thoroughly whether the so called household exception applies which exempts users from qualifying as controller. However, this issue is beyond the scope of this opinion.

[11] e.g. Level of instructions, monitoring by the cloud client, expertise of the parties

[12] Opinion1/2010on the concepts of "controller" and "processor" - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

Cloud providers (as processors) have a duty to ensure confidentiality. Directive 95/46 EC states that: *"Any persons acting under the authority of the controller or of the processor, including the processors themselves, who have access to personal data must not process them except on instructions from the controller, unless he is required to do so by law."* Access to data by the cloud provider during its provision of services is also fundamentally governed by the requirement to comply with the provisions of Article 17 of the Directive – see section 3.4.2.

Processors must take into account the type of cloud in question (public, private, community or hybrid / IaaS, SaaS or PaaS [see Annex a) Rollout models - b) Service Provision Models]) and the type of service contracted by the client. Processors are responsible for adopting security measures in line with those in EU legislation as applied in the controller's and the processor's jurisdictions. Processors must also support and assist the controller in complying with (exercised) data subjects' rights.

3.3.2 Subcontractors

Cloud computing services may entail the involvement of a number of contracted parties who act as processors. It is also common for processors to subcontract additional sub-processors which then gain access to personal data. If processors subcontract services out to sub-processors, they are obliged to make this information available to the client, detailing the type of service subcontracted, the characteristics of current or potential sub-contractors and guarantees that these entities offer to the provider of cloud computing services to comply with Directive 95/46/EC.

All the relevant obligations must therefore apply also to the sub-processors through contracts between the cloud provider and subcontractor reflecting the stipulations of the contract between cloud client and cloud provider. In its Opinion 1/2010 on the concepts of "controller" and "processor", the Article 29 Working Party referred to the multiplicity of processors in cases in which processors may have a direct relationship with the controller or operate as subcontractors where the processors outsource part of the processing work they had been tasked with. "*Nothing in the Directive prevents that on account of organisational requirements, several entities may be designated as processors or (sub-)processors also by subdividing the relevant tasks. However, all of them are to abide by the instructions given by the controller in carrying out the processing.*"[13].

In such scenarios, the obligations and responsibilities deriving from data protection legislation should be set out clearly and not dispersed throughout the chain of outsourcing or subcontracting, in order to ensure effective control over and allocate clear responsibility for processing activities.

A possible model of assurances that can be used to clarify the duties and obligations of processors when they subcontract data processing was first introduced by the Commission Decision of 5 February 2010 on the standard contractual clauses for the transfer of personal data to processors established in third countries[14]. In this model sub-processing is permitted only with the prior written consent of the controller and with a written agreement imposing the same obligations on the sub-processor as are imposed on the processor. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the

[13] Cf. WP169, p. 29, Opinion 1/2010on the concepts of "controller" and "processor" (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf)[14] See FAQ II.5 of WP176.

processor shall remain fully liable to the controller for the performance of the sub-processor's obligations under such agreement. A provision of this kind could be used in any contractual clauses between a controller and a cloud service provider, where the latter intends to provide services through subcontracting, to assure required guarantees for the sub-processing.

A similar solution regarding assurances in the course of sub-processing has been proposed recently by the Commission in the proposal for a General Data Protection Regulation[15]. The acts of a processor must be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that, among other requirements, the processor shall enlist another processor only with the prior permission of the controller (Article 26(2) of the proposal).

In the view of the WP29, the processor can subcontract its activities only on the basis of the consent of the controller, which may be generally given at the beginning of the service[16] with a clear duty for the processor to inform the controller of any intended changes concerning the addition or replacement of subcontractors with the controller retaining at all times the possibility to object to such changes or to terminate the contract. There should be a clear obligation of the cloud provider to name all the subcontractors commissioned. In addition, a contract should be signed between cloud provider and subcontractor reflecting the stipulations of the contract between cloud client and cloud provider. The controller should be able to avail of contractual recourse possibilities in case of breaches of contracts caused by the sub-processors. This could be arranged by ensuring that the processor is directly liable toward the controller for any breaches caused by any sub-processors he has enlisted, or through the creation of third party beneficiary right for the benefit of the controller in the contracts signed between the processor and the sub-processors or by the fact that those contracts will be signed on behalf of the data controller, making this later a party to the contract.

3.4 Data protection requirements in the client-provider relationship

3.4.1 Compliance with basic principles

The lawfulness of the processing of personal data in the cloud depends on the adherence to basic principles of EU data protection law: Namely, transparency vis-à-vis the data subject is to be guaranteed, the principle of purpose specification and limitation must be complied with and personal data must be erased as soon as their retention is not necessary any more. Moreover, appropriate technical and organisational measures must be implemented to ensure an adequate level of data protection and data security.

3.4.1.1 Transparency

Transparency is of key importance for a fair and legitimate processing of personal data. Directive 95/46/EC obliges the cloud client to provide a data subject from whom data relating to himself are collected with information on his identity and the purpose of the processing. The cloud client should also provide any further information such as on the recipients or categories of recipients of the data, which can also include processors and sub-processors in

[15] Proposal for a Regualtion of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 25.1.2012.

so far as such further information is necessary to guarantee fair processing in respect of the data subject (cf. Article 10 of the Directive)[17].

Transparency must also be ensured in the relationship(s) between cloud client, cloud provider and subcontractors (if any). The cloud client is only capable of assessing the lawfulness of the processing of personal data in the cloud if the provider informs the client about all relevant issues. A controller contemplating engaging a cloud provider should carefully check the cloud provider's terms and conditions and assess them from a data protection point of view.

Transparency in the cloud means it is necessary for the cloud client to be made aware of all subcontractors contributing to the provision of the respective cloud service as well as of the locations of all data centres personal data may be processed at.[18]

If the provision of the service requires the installation of software on the cloud client's systems (e.g., browser plug-ins), the cloud provider should as a matter of good practice inform the client about this circumstance and in particular about its implications from a data protection and data security point of view. Vice versa, the cloud client should raise this matter ex ante, if it is not addressed sufficiently by the cloud provider.

3.4.1.2 Purpose specification and limitation

The principle of purpose specification and limitation requires that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (cf. Article 6(b) of Directive 95/46/EC). The cloud client must determine the purpose(s) of the processing prior to the collection of personal data from the data subject and inform the data subject thereof. The cloud client must not process personal data for other purposes that are not compatible with the original ones.

Moreover, it must be ensured that personal data are not (illegally) processed for further purposes by the cloud provider or one of his subcontractors. As a typical cloud scenario may easily involve a larger number of subcontractors, the risk of processing of personal data for further, incompatible purposes must therefore be assessed as being quite high. To minimise this risk, the contract between cloud provider and cloud client should include technical and organisational measures to mitigate this risk and provide assurances for the logging and auditing of relevant processing operations on personal data that are performed by employees of the cloud provider or the subcontractors.[19] Penalties should be imposed in the contract against the provider or subcontractor if data protection legislation is breached.

3.4.1.3 Erasure of data

According to Article 6(e) of Directive 95/46/EC, personal data must be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Personal data that are not necessary any more must be erased or truly anonymised. If this data cannot be erased due to legal retention rules (e.g., tax regulations), access to this personal data should be blocked. It

[17] A corresponding duty to inform the data subject exists when data that have not been obtained from the data subject himself, but from different sources are recorded or disclosed to a third party (cf. Article 11).

[18] Only then he will be able to assess whether personal data may be transferred to a so-called third country outside of the European Economic Area (EEA) which does not ensure an adequate level of protection within the meaning of Directive 95/46/EC.

[19] Cf. section 3.4.3 below.

is the cloud client's responsibility to ensure that personal data are erased as soon as they are not necessary in the aforementioned sense any more[20].

The principle of erasure of data applies to personal data regardless of whether they are stored on hard drives or on other storage media (e.g., backup tapes). Since personal data may be kept redundantly on different servers at different locations, it must be ensured that each instance of them is erased irretrievably (i.e., previous versions, temporary files and even file fragments are to be deleted as well).

Cloud clients must be aware of the fact that log data[21] facilitating auditability of, e.g., storage, modifications or erasure of data may also qualify as personal data relating to the person who initiated the respective processing operation.[22]

Secure erasure of personal data requires that either the storage media to be destroyed or demagnetised or the stored personal data is deleted effectively through overwriting. For the overwriting of personal data, special software tools that overwrite data multiple times in accordance with a recognised specification should be used.

The cloud client should make sure that the cloud provider ensures secure erasure in the abovementioned sense and that the contract between the provider and the client contains clear provision for the erasure of personal data[23]. The same holds true for contracts between cloud providers and subcontractors.

3.4.2 Contractual safeguards of the "controller"-"processor" relationship(s)

Where controllers decide to contract cloud computing services, they are required to choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures (Article 17(2) of Directive 95/46/EC). Furthermore, they are legally obliged to sign a formal contract with the cloud service provider, as stated in Article 17(3) of Directive 95/46/EC. This article establishes the requirement for there to be a contract or other binding legal act to govern the relationship between the controller and the processor. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the technical and organizational measures shall be in writing or in another equivalent form.

The contract must at a minimum establish the fact, in particular, that the processor is to follow the instructions of the controller and that the processor must implement technical and organizational measures to adequately protect personal data.

To ensure legal certainty the contract should also set forth the following issues:

1. Details on the (extent and modalities of the) client's instructions to be issued to the provider, with particular regard to the applicable SLAs (which should be objective and measurable) and the relevant penalties (financial or otherwise including the ability to sue the provider in case of non-compliance).
2. Specification of security measures that the cloud provider must comply with, depending on the risks represented by the processing and the nature of the data to be

[20] Erasure of data is an issue both throughout the duration of a cloud computing contract and upon its termination. It is also relevant in case of substitution or withdrawal of a subcontractor.

[21] Remarks on logging requirements are provided below at 4.3.4.2.

[22] This means that reasonable retention periods for log files are to be defined and that processes safeguarding the timely erasure or anonymisation of these data are to be in place.

[23] Cf. section 3.4.3 below.

protected. It is of great importance that concrete technical and organizational measures are specified such as those outlined in paragraph 3.4.3 below. This is without prejudice to the application of more stringent measures, if any, that may be envisaged under the client's national law.

3. Subject and time frame of the cloud service to be provided by the cloud provider, extent, manner and purpose of the processing of personal data by the cloud provider as well as the types of personal data processed.
4. Specification of the conditions for returning the (personal) data or destroying the data once the service is concluded. Furthermore, it must be ensured that personal data are erased securely at the request of the cloud client.
5. Inclusion of a confidentiality clause, binding both upon the cloud provider and any of its employees who may be able to access the data. Only authorized persons can have access to data.
6. Obligation on the provider's part to support the client in facilitating exercise of data subjects' rights to access, correct or delete their data.
7. The contract should expressly establish that the cloud provider may not communicate the data to third parties, even for preservation purposes unless it is provided for in the contract that there will be subcontractors. The contract should specify that sub-processors may only be commissioned on the basis of a consent that can be generally given by the controller in line with a clear duty for the processor to inform the controller of any intended changes in this regard with the controller retaining at all times the possibility to object to such changes or to terminate the contract. There should be a clear obligation of the cloud provider to name all the subcontractors commissioned (e.g., in a public digital register). It must be ensured that contracts between cloud provider and subcontractor reflect the stipulations of the contract between cloud client and cloud provider (i.e. that sub-processors are subject to the same contractual duties than the cloud provider). In particular, it must be guaranteed that both cloud provider and all subcontractors shall act only on instructions from the cloud client. As explained in the chapter on sub-processing the chain of liability should be clearly set in the contract. It should set out the obligation on the part of the processor to frame international transfers, for instance by signing contracts with sub-processors, based on the 2010/87/EU standard contractual clauses.
8. Clarification of the responsibilities of the cloud provider to notify the cloud client in the event of any data breach which affects the cloud client's data.
9. Obligation of the cloud provider to provide a list of locations in which the data may be processed.
10. The controller's rights to monitor and the cloud provider's corresponding obligations to cooperate.
11. It should be contractually fixed that the cloud provider must inform the client about relevant changes concerning the respective cloud service such as the implementation of additional functions.
12. The contract should provide for logging and auditing of relevant processing operations on personal data that are performed by the cloud provider or the subcontractors.
13. Notification of cloud client about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a

prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

14. A general obligation on the provider's part to give assurance that its internal organisation and data processing arrangements (and those of its sub-processors, if any) are compliant with the applicable national and international legal requirements and standards.

In the event of infringement by the controller, any person suffering damages as a result of unlawful processing shall have the right to receive compensation from the controller for the damages caused. Should the processors use the data for any other purpose, or communicate them or use them in a way that breaches the contract, they shall also be considered to be controllers, and shall be held liable for the infringements in which they were personally involved.

It should be noted that, in many cases, cloud service providers offer standard services and contracts to be signed by controllers, which set forth a standard format for processing personal data. This imbalance in the contractual power of a small controller with respect to large service providers should not be considered as justification for the controllers to accept clauses and terms of contracts which are not in compliance with data protection law.

3.4.3 Technical and organisational measures of data protection and data security

Article 17(2) of Directive 95/46/EC puts full responsibility on cloud clients (acting as data controllers) to choose cloud providers that implement adequate technical and organisational security measures to protect personal data and to be able to demonstrate accountability.

In addition to the core security objectives of availability, confidentiality and integrity, attention must also be drawn to the complementary data protection goals of transparency (see 3.4.1.1 above), isolation [24], intervenability, accountability and portability. This section highlights these central data protection goals, without prejudice to other complementary security oriented risk analysis[25].

3.4.3.1 Availability

Providing availability means ensuring timely and reliable access to personal data.

One severe threat to availability in the cloud is accidental loss of network connectivity between the client and the provider or of server performance caused by malicious actions such as (Distributed) Denial of Service (DoS)[26] attacks. Other availability risks include accidental hardware failures both on the network and in the cloud processing and data storage systems, power failures and other infrastructure problems.

Data controllers should check whether the cloud provider has adopted reasonable measures to cope with the risk of disruptions, such as backup internet network links, redundant storage and effective data backup mechanisms.

---

[24] In Germany the broader concept of "unlinkability" has been introduced into legislation and is promoted by the Conference of Data Protection Commissioners.

[25] Cf. e.g. ENISA at http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[26] A DoS attack is a coordinated attempt to make a computer or network resource unavailable to its authorised users, either temporarily or indefinitely (e.g., by means of a large number of attacking systems paralysing their target with a multitude of external communication requests).

3.4.3.2 Integrity

Integrity may be defined as the property that data is authentic and has not been maliciously or accidentally altered during processing, storage or transmission. The notion of integrity can be extended to IT systems and requires that the processing of personal data on these systems remains unaltered.

Detecting alterations to personal data can be achieved by cryptographic authentication mechanisms such as message authentication codes or signatures.

Interference with the integrity of IT systems in the cloud can be prevented or detected by means of intrusion detection / prevention systems (IPS / IDS). This is particularly important in the type of open network environments in which clouds usually operate.

3.4.3.3 Confidentiality

In a cloud environment, encryption may significantly contribute to the confidentiality of personal data if implemented correctly, although it does not render personal data irreversibly anonymous[27]. Encryption of personal data should be used in all cases when "in transit" and when available to data "at rest".[28] In some cases (e.g., an IaaS storage service) a cloud client may not rely on an encryption solution offered by the cloud provider, but may choose to encrypt personal data prior to sending them to the cloud. Encrypting data at rest requires particular attention to cryptographic key management as data security then ultimately depends on the confidentiality of the encryption keys.

Communications between cloud provider and client as well as between data centres should be encrypted. Remote administration of the cloud platform should only take place via a secure communication channel. If a client plans to not only store, but also further process personal data in the cloud (e.g., searching databases for records), he must bear in mind that encryption cannot be maintained during processing of the data (except of very specific computations).

Further technical measures aiming at ensuring confidentiality include authorization mechanisms and strong authentication (e.g. two-factor authentication). Contractual clauses should also impose confidentiality obligations on employees of cloud clients, cloud providers and subcontractors.

3.4.3.4 Transparency

Technical and organisational measures must support transparency to allow review, cf. 3.4.1.1.

3.4.3.5 Isolation (purpose limitation)

In cloud infrastructures, resources such as storage, memory and networks are shared among many tenants. This creates new risks for data to be disclosed and processed for illegitimate purposes. The protection goal "isolation" is meant to address this issue and contribute to guarantying that data is not used beyond its initial purpose (Article 6(b) of Dir 95/46/EC) and to maintain confidentiality and integrity.[29]

---

[27] Directive 95/46/EC - Recital 26: "(...); whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; (...)". I n the same line, the technical data fragmentation processes that may be used in the framework of the provision of CC services will not lead to irreversible anonymisation and thus does not imply that data protection obligations do not apply.

[28] This holds true in particular for data controllers who plan to transfer sensitive data in the meaning of Article 8 of Directive 95/46/EC (e.g., health data) to the cloud or who are subject to specific legal obligations of professional secrecy.

[29] Cf. 3.4.1.2.

Achieving isolation first requires adequate governance of the rights and roles for accessing personal data, which is reviewed on a regular basis. The implementation of roles with excessive privileges should be avoided (e.g., no user or administrator should be authorised to access the entire cloud). More generally, administrators and users must only be able to access the information that is necessary for their legitimate purposes (least privilege principle).

Secondly, isolation also depends on technical measures such as the hardening of hypervisors and proper management of shared resources if virtual machines are used to share physical resources between different cloud customers. .

3.4.3.5 Intervenability

Directive 95/46/EC gives the data subject the rights of access, rectification, erasure, blocking and objection (cf. Article 12 and 14). The cloud client must verify that the cloud provider does not impose technical and organisational obstacles to these requirements, including in cases when data is further processed by subcontractors.

The contract between the client and the provider should stipulate that the cloud provider is obliged to support the client in facilitating exercise of data subjects' rights and to ensure that the same holds true for his relation to any subcontractor.[30]

3.4.3.6 Portability

Currently, most cloud providers do not make use of standard data formats and service interfaces facilitating interoperability and portability between different cloud providers. If a cloud client decides to migrate from one cloud provider to another, this lack of interoperability may result in the impossibility or at least difficulties to transfer the client's (personal) data to the new cloud provider (so-called vendor lock-in). The same holds true for services that the client developed on a platform offered by the original cloud provider (PaaS). The cloud client should check whether and how the provider guarantees the portability of data and services prior to ordering a cloud service.[31]

3.4.4.7 Accountability

In IT accountability can be defined as the ability to establish what an entity did at a certain point in time in the past and how. In the field of data protection it often takes a broader meaning and describes the ability of parties to demonstrate that they took appropriate steps to ensure that data protection principles have been implemented.

IT accountability is particularly important in order to investigate personal data breaches, where cloud clients, providers and sub-processor may each bear a degree of operational responsibility. The ability for the cloud platform to provide reliable monitoring and comprehensive logging mechanisms is of paramount importance in this regard.

Moreover, cloud providers should provide documentary evidence of appropriate and effective measures that deliver the outcomes of the data protection principles outlined in the previous sections. Procedures to ensure the identification of all data processing operations, to respond to access requests, the allocation of resources including the designation of data protection

---

[30] Cf. section 3.4.5 No. 7 above. The provider may even be instructed to answer requests on behalf of the client.

[31] Preferably, the provider should make use of standardised or open data formats and interfaces. In any event, contractual clauses stipulating assured formats, preservation of logical relations and any costs accruing from the migration to another cloud provider should be agreed on.

officers who are responsible for the organisation of data protection compliance, or independent certification procedures are examples of such measures. In addition, data controllers should ensure that they are prepared to demonstrate the setting up of the necessary measures to the competent supervisory authority upon request.[32]

3.5 International transfers

Article 25 and 26 of the Directive 95/46/EC provide for free flow of personal data to countries located outside the EEA only if that country or the recipient provides an adequate level of data protection. Otherwise specific safeguards must be put in place by the controller and its co-controllers and/or processors. However, cloud computing is most frequently based on a complete lack of any stable location of data within the cloud provider's network. Data can be in one data centre at 2pm and on the other side of the world at 4pm. The cloud client is therefore rarely in a position to be able to know in real time where the data are located or stored or transferred. In this context, the traditional legal instruments providing a framework to regulate data transfers to non-EU third countries not providing adequate protection, have limitations.

3.5.1 Safe Harbor and adequate countries

Adequacy findings, including Safe Harbor, are limited in respect of the geographical scope, and therefore do not cover all transfers within the Cloud.
Transfers to US organizations adhering to the principles can take place lawfully under EU law since the recipient organizations are deemed to provide an adequate level of protection to the transferred data.

However, in the view of the Working Party, sole self-certification with Safe Harbor may not be deemed sufficient in the absence of robust enforcement of data protection principles in the cloud environment. In addition, Article 17 of the EU directive requires a contract to be signed from a controller to a processor for processing purposes, which is confirmed in FAQ 10 of the EU-US Safe Harbor Framework documents. This contract is not subject to prior authorization from the European DPAs. Such contract specifies the processing to be carried out and any measures necessary to ensure that the data are kept secure. Different national legislations and DPAs may have additional requirements.

The Working Party considers that companies exporting data should not merely rely on the statement of the data importer claiming that he has a Safe Harbor certification. On the contrary, the company exporting data should obtain evidence that the Safe Harbor self-certifications exists and request evidence demonstrating that their principles are complied with. This is important especially with regard to the information provided to data subjects affected by the data processing[33, 34].

The Working Party also considers that cloud client must verify if the standard contracts composed by cloud providers are compliant with national requirements regarding contractual data processing. National legislation may require sub-processing to be defined in the contract,

---

[32] The Working Party provided detailed remarks on the topic of accountability in its Opinion 3/2010 on the principle of accountability http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.

[33] See German DPA: http://www.datenschutz-berlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf.

[34] For requirements regarding contracting sub-processors, see 3.3.2.

which includes the locations and other data on sub-processors, and traceability of the data. Normally the cloud providers do not offer the client such information – their commitment to the Safe Harbor cannot substitute for the lack of the above guarantees when required by the national legislation. In such cases the exporter is encouraged to use other legal instruments available, such as standard contractual clauses or BCR.

Finally, the Working Party considers that the Safe Harbor principles by themselves may also not guarantee the data exporter the necessary means to ensure that appropriate security measures have been applied by the cloud provider in the US, as may be required by national legislations based on the Directive 95/46/EC[35]. In terms of data security cloud computing raises several cloud-specific security risks, such as loss of governance, insecure or incomplete data deletion, insufficient audit trails or isolation failures[36], which are not sufficiently addressed by the existing Safe Harbor principles on data security[37]. Additional safeguards for data security may thus be deployed; such as by incorporating the expertise and resources of third parties that are capable of assessing the adequacy of cloud providers through different auditing, standardization and certification schemes[38]. For these reasons it might be advisable to complement the commitment of the data importer to the Safe Harbor with additional safeguards taking into account the specific nature of the cloud.

3.5.2 Exemptions

The exemptions provided by article 26 of the EU Directive 95/46 enable data exporters to transfer data out of the EU without providing additional guarantees. However, WP29 has adopted an opinion in which it considered that exemptions shall apply only where transfers are neither recurrent, nor massive or structural.[39]

Based on such interpretations, it is almost impossible to rely on exemptions in the context of cloud computing.

3.5.3 Standard contractual clauses

Standard contractual clauses as adopted by the EU Commission for the purpose of framing international data transfers between two controllers or one controller and a processor are based on a bilateral approach. When the cloud provider is considered to be the processor, model clauses 2010/87/EC are an instrument that can be used between the processor and the controller as a basis for the cloud computing environment to offer adequate safeguards in the context of international transfers.

In addition to the standard contractual clauses, the Working Party considers that cloud providers could offer customers provisions that build on their pragmatic experiences as long as they do not contradict, directly or indirectly the standard contractual clauses approved by

---

35 See an opinion by the Danish DPA: http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution.

36 Described in detail in ENISA paper Cloud Computing: Benefits, Risks and Recommendations for Information Security at: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

37 "Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction."

38 See section 4.2 below.

39 Working Document 12/1998: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, Adopted by the Working Party on 24 July 1998 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf).

the Commission or prejudice fundamental rights or freedoms of the data subjects[40]. Nevertheless, the companies may not amend or change the standard contractual clauses without implying that the clauses will no longer be "standard"[41].

When the cloud provider acting as processor is established in the EU, the situation might be more complex since the model clauses applies, in general, only to the transfer of data from a EU controller to a non EU processor (see recital 23 of the Commission decision on the model Clauses 2010/87/EU and WP 176).

As regards the contractual relationship between the non EU processor and the sub-processors, a written agreement which imposes the same obligations on the subprocessor as are imposed on the processor in the Model clauses should be put in place.

3.5.4 BCR: towards a global approach

BCR constitute a code of conduct for companies which transfer data within their group. Such solution will be provided also for the context of cloud computing when the provider is a processor. Indeed, WP29 is currently working on BCRs for processors which will allow the transfer within the group for the benefit of the controllers without requiring the signature of contracts between processor and subprocessors per client.[42]

Such BCR for processors would enable the provider's client to entrust their personal data to the processor while being assured that the data transferred within the provider's business scope would receive an adequate level of protection.

4. Conclusions and recommendations

Businesses and administrations wishing to use cloud computing should conduct, as a first step, a comprehensive and thorough risk analysis. This analysis must address the risks related to processing of data in the cloud (lack of control and insufficient information – see section 2 above) by having regard to the type of data processed in the cloud.[43] Special attention should also be paid to assessing the legal risks regarding data protection, which concern mainly security obligations and international transfers. The processing of sensitive data via cloud computing raises additional concerns. Therefore without prejudice to national laws such processing requires additional safeguards.[44] The conclusions below are meant to provide a checklist for data protection compliance by cloud clients and cloud providers based on the current legal framework; some recommendations are also provided with a view to future developments in the regulatory framework at EU level and beyond.

[40] See FAQ IV B1.9 9, Can companies include the standard contractual clauses in a wider contract and add specific clauses? published by the EC on http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

[41] See FAQ IV B1.10, Can Companies amend and change the standard contractual clauses approved by the Commission?

[42] See Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, adopted on 6th June 2012: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf

[43] ENISA provides a list of the risks that must be taken into consideration http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

[44] See Sopot Memorandum, cf. footnote 2 above.

4.1 Guidelines for clients and providers of cloud computing services

-Controller-processor relationship: This Opinion focuses on the client-provider relationship as controller-processor relationship; (see paragraph 3.3.1); Nevertheless based on concrete circumstances situations may exist where the cloud provider acts as a controller as well, e.g. when the provider re-processes some personal data for its own purposes. In such a case, the cloud provider has full (joint) responsibility for the processing and must fulfil all legal obligations that are stipulated by Directives 95/46/EC and 2002/58/EC (if applicable);

-Cloud client's responsibility as a controller: The client as the controller must accept responsibility for abiding by data protection legislation and is subject to all the legal obligations mentioned in Directive 95/46/EC and 2002/58/EC, where applicable, in particular vis-à-vis data subjects (see 3.3.1). The client should select a cloud provider that guarantees compliance with EU data protection legislation as reflected by the appropriate contractual safeguards summed up below;

-Subcontracting safeguards: Provisions for subcontractors should be provided for in any contract between the cloud provider and cloud clients. The contract should specify that sub-processors may only be commissioned on the basis of a consent that can be generally given by the controller in line with a clear duty for the processor to inform the controller of any intended changes in this regard with the controller retaining at all times the possibility to object to such changes or to terminate the contract. There should be a clear obligation of the cloud provider to name all the subcontractors commissioned. The cloud provider should sign a contract with each subcontractor reflecting the stipulations of his contract with the cloud client; the client should ensure that it has contractual recourse possibilities in case of contractual breaches by the provider's sub-contractors (see 3.3.2);

-Compliance with fundamental data protection principles:

- Transparency (see 3.4.1.1): cloud providers should inform cloud clients about all (data protection) relevant aspects of their services during contract negotiations; in particular, clients should be informed about all subcontractors contributing to the provision of the respective cloud service and all locations in which data may be stored or processed by the cloud provider and/or its subcontractors (notably, if some or all locations are outside of the European Economic Area (EEA)); the client should be provided with meaningful information about technical and organisational measures implemented by the provider; the client should as a matter of good practice inform data subjects about the cloud provider and all subcontractors (if any) as well as about locations in which data may be stored or processed by the cloud provider and/or its subcontractors;
- Purpose specification and limitation (3.4.1.2): the client should ensure compliance with purpose specification and limitation principles and ensure that no data is processed for further purposes by the provider or any subcontractors. Commitments in this respect should be captured in the appropriate contractual measures (including technical and organisational safeguards);
- Data retention (3.4.1.3): the client is responsible for ensuring that personal data are erased (by the provider and any subcontractors) from wherever they are stored as soon as they are no longer necessary for the specific purposes; secure

erasure mechanisms (destruction, demagnetisation, overwriting) should be provided for contractually;

- Contractual safeguards (see 3.4.2, 3.4.3 and 3.5):
    - In general: the contract with the provider (and the ones to be stipulated between provider and sub-contractors) should afford sufficient guarantees in terms of technical security and organizational measures (under Article 17(2) of the directive) and should be in writing or in another equivalent form. The contract should detail the client's instructions to the provider including subject and time frame of the service, objective and measurable service levels and the relevant penalties (financial or otherwise); it should specify the security measures to be complied with as a function of the risks of the processing and the nature of the data, in line with the requirements made below and subject to more stringent measures as envisaged under the client's national law; if cloud providers aim at making use of standard contractual terms, they should ensure that these terms comply with data protection requirements (see 3.4.2); in particular technical and organisational measures that have been implemented by the provider should be specified in the respective terms;
    - Access to data: only authorised persons should have access to the data; a confidentiality clause should be included in the contract vis-à-vis the provider and its employees;
    - Disclosure of data to third parties: this should be regulated only via the contract, which should include an obligation for the provider to name all its sub-contractors – e.g. in a public digital register – and ensure access to information for the client of any changes in order to enable him to object to those changes or terminate the contract; the contract should also require the provider to notify any legally binding request for disclosure of the personal data by a law enforcement authority, unless such disclosure is otherwise prohibited; the client should warrant that the provider will reject any non-legally binding requests for disclosure;
    - Obligations to co-operate: client should ensure that the provider is obliged to co-operate with regard to the client's right to monitor processing operations, facilitate the exercise of data subjects' rights to access/correct/erase their data, and (where applicable) notify the cloud client of any data breaches affecting client's data;
    - Cross-border data transfers: The cloud client should verify if the cloud provider can guarantee lawfulness of cross-border data transfers and limit the transfers to countries chosen by the client, if possible. Transfers of data to non-adequate third countries require specific safeguards via the use of Safe Harbor arrangements, standard contractual clauses (SCC) or binding corporate rules (BCR) as appropriate; the use of SCC for processors (under Commission's decision 2010/87/EC) requires certain adaptations to the cloud environment (to prevent having separate per-client contracts between a provider and its sub-processors) which might imply the need for prior authorisation from the competent DPA; a list of the locations in which the service may be provided should be included in the contract;
    - Logging and auditing of processing: the client should request logging of processing operations performed by the provider and its sub-contractors; the client should be empowered to audit such processing operations, however

third-party audits chosen by the controller and certification may also be acceptable providing full transparency is guaranteed (e.g. by providing for the possibility to obtain a copy of a third-party audit certificate or a copy of the audit report verifying certification);

- Technical and organisational measures: these should be aimed at remedying the risks entailed by lack of control and lack of information that feature most prominently in the cloud computing environment. The former include measures aimed at ensuring availability, integrity, confidentiality, isolation, intervenability and portability as defined in the paper whilst the latter focus on transparency (see 3.4.3 for full details).

4.2 Third Party Data Protection Certifications

- Independent verification or certification by a reputable third party can be a credible means for cloud providers to demonstrate their compliance with their obligations as specified in this Opinion. Such certification would, as a minimum, indicate that data protection controls have been subject to audit or review against a recognised standard meeting the requirements set out in this Opinion by a reputable third party organisation.[45] In the context of cloud computing, potential customers should look to see whether cloud services providers can provide a copy of this third party audit certificate or indeed a copy of the audit report verifying the certification including with respect to the requirements set out in this Opinion.
- Individual audits of data hosted in a multi-party, virtualised server environment may be impractical technically and can in some instances serve to increase risks to those physical and logical network security controls in place. In such cases, a relevant third party audit chosen by the controller may be deemed to satisfy in lieu of an individual controller's right to audit.
- The adoption of privacy-specific standards and certifications is central to the establishment of a trustworthy relationship between cloud providers, controllers and data subjects.
- These standards and certifications should address technical measures (such as localisation of data or encryption) as well as processes within cloud providers' organisation that guarantee data protection (such as access control policies, access control or backups).

4.3 Recommendations: Future Developments

The WP is fully aware that the complexities of cloud computing cannot be addressed completely via the safeguards and solutions outlined in this Opinion, which provide, however, a sound basis for securing the processing of personal data that EEA-based clients submit to cloud providers. This section is meant to highlight some issues that need to be tackled in the short to medium term to enhance the safeguards in place, assisting the cloud industry in terms of the issues highlighted whilst ensuring respect for the fundamental rights to privacy and data protection.

[45] Such standards would include those issued by the International Standards Organisation, the International Auditing and Assurance Standards Board and the Auditing Standards Board of the American Institute of Certified Public Accountants in so far as these organisations provide standards that meet the requirements set out in this opinion.

- Better balancing of responsibilities between controller and processor: The WP welcomes the provisions contained in Article 26 of the Commission's proposals (Draft EU General Data Protection Regulation) that are aimed at making processors more accountable towards controllers by assisting them in ensuring compliance in particular with security and related obligations. Article 30 of the proposal introduces a legal obligation for the processor to implement appropriate technical and organisational measures. The draft proposals clarify that a processor failing to comply with the controller's instructions qualifies as a controller and is subject to specific joint controllership rules. The Article 29 Working party considers that this proposal goes in the right direction to remedy the unbalance that is often a feature in the cloud computing environment, where the client (especially if it is a SME) may find it difficult to exercise the full control required by data protection legislation on how the provider delivers the requested services. Furthermore, in view of the asymmetric legal position of data subjects and small business users *vis á vis* big cloud computing providers, a more proactive role for consumer and business interest organisations is recommended in order to negotiate more balanced general terms and conditions of such companies.

- Access to personal data for national security and law enforcement purposes: It is of the utmost importance to add to the future Regulation that controllers operating in the EU must be prohibited from disclosing personal data to a third country if so requested by a third country's judicial or administrative authority, unless this is expressly authorized by an international agreement or provided for by mutual legal assistance treaties or approved by a supervisory authority. Council Regulation (EC) No 2271/96 is an appropriate example of legal ground for this.[46] The Working Party is concerned by this gap in the Commission proposal as it entails a considerable loss of legal certainty for the data subjects whose personal data are stored in data centres all over the world. For that reason, the Working Party would like to stress[47] the need to include in the Regulation the obligatory use of Mutual Legal Assistance Treaties (MLATs) in case of disclosures not authorised by Union or Member States law.

- Special precautions by the public sector: A special caveat is to be added as to the need for a public body to first assess whether the communication, processing and storage of data outside national territory may expose the security and privacy of citizens and national security and economy to unacceptable risks – in particular if sensitive databases (e.g. census data) and services (e.g. health care.) are involved.[48] This special consideration should be given, at any rate, whenever sensitive data are processed in the Cloud context. From this standpoint, consideration might be given by national governments and European Union institutions to further investigate the concept of a European Governmental cloud as a supra national virtual space where a consistent and harmonized set of rules could be applied.

---

[46] Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom, Official Journal L 309 , 29/11/1996 P. 0001 - 0006, URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996R2271:EN:HTML

[47] Cf. WP 191 - Opinion 01/2012 on the data protection reform proposals, page 23.

[48] In this respect, ENISA makes the following recommendation in its paper on Security & Resilience in Governmental Clouds (http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/at_download/fullReport): "In terms of architecture, for sensitive applications private and community clouds appear to be the solution that currently best fits the needs of public administrations since they offer the highest level of governance, control and visibility, even though when planning a private or community cloud, special regard should be given to the scale of the infrastructure."

- European Cloud Partnership: The Working Party supports the European Cloud Partnership (ECP) strategy presented by Mrs Kroes, Vice-president of the European Commission, in January 2012 at Davos.[49] This strategy involves public IT procurement to stimulate a European cloud market. Transferring personal data to a European cloud provider, sovereignly governed by European data protection law, could bring great data protection advantages to customers, in particular by fostering the adoption of common standards (especially in terms of interoperability and data portability) as well as legal certainty.

[49] Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda, Setting up the European Cloud Partnership World Economic Forum Davos, Switzerland, 26th January 2012, URL: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/1 23.

ANNEX

a) Rollout models

Private cloud[50] describes an IT infrastructure that is dedicated to an individual organization; it is located at the organization's premises or else its management is outsourced to a third party (usually via server hosting) that is under the controller's strict authority. A private cloud can be compared to a conventional data centre – the difference being that technological arrangements are implemented to optimize use of the available resources and enhance those resources via small investments that are made in a stepwise fashion over time.

Public cloud, conversely, is an infrastructure owned by a provider specializing in the supply of services that makes available – and therefore shares – his systems to/among users, businesses and/or public administrative bodies. The services can be accessed via the Internet, which entails transferring data processing operations and/or the data to the service provider's systems. Therefore the service provider takes on a key role as regards to the effective protection of the data committed to his systems. Along with the data, a user is bound to transfer a major portion of his control over those data.

Alongside "public" and "private" clouds, there are so-called "intermediate" or "hybrid" clouds where services provided by private infrastructures co-exist with services purchased from public clouds. Reference should also be made to the "community clouds", where the IT infrastructure is shared by several organizations for the benefit of a specific user community.

Flexibility and simplicity in configuring cloud systems allow their "elastic" dimensioning, i.e. these systems can be adjusted to the specific requirements in accordance with a usage-based approach. Users do not have to manage any IT systems, which are relied upon on the basis of outsourcing agreements and therefore are handled in full by the third party in whose cloud the data are stored. It is often the case that large-sized providers with complex infrastructures come into play; this is why the cloud might span several locations and users might ignore where exactly their data are being stored.

b) Service provision models

Depending on user requirements, there are several cloud computing solutions available on the market; they can be grouped into three main categories or "service models". These models usually apply to both private and public cloud solutions:

---

[50] The NIST (National Institute of Standards and Technology) in the US, which has been working for some years on standardization of cloud-based technologies[50], and whose definitions are also referred to in ENISA's paper:
Private cloud.
The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. It should be pointed out that a "private cloud" relies on at least certain technologies that are also typical of "public clouds" – including, in particular, virtualization technologies that foster the re-organisation (or overhaul) of the data processing architecture as explained above.
Public cloud.
The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services

- **IaaS (Cloud Infrastructure as a Service):** a provider leases a technological infrastructure, i.e. virtual remote servers the end-user can rely upon in accordance with mechanisms and arrangements such as to make it simple, effective as well as beneficial to replace the corporate IT systems at the company's premises and/or use the leased infrastructure alongside the corporate systems. Such providers are usually specialized market players and can rely actually on a physical, complex infrastructure that often spans over several geographic areas.
- **SaaS (Cloud Software as a Service):** a provider delivers, via the web, various application services and makes them available to end-users. These services are often meant to replace conventional applications to be installed by users on their local systems; accordingly, users are ultimately meant to outsource their data to the individual provider. This is the case, for instance, of typical web-based office applications such as spreadsheets, text processing tools, computerized registries and agendas, shared calendars, etc.; however, the services in question also include cloud-based email applications.
- **PaaS (Cloud Platform as a Service):** a provider offers solutions for the advanced development and hosting of applications. These services are usually addressed to market players that use them to develop and host proprietary application-based solutions to meet in-house requirements and/or to provide services to third parties. Again, the services delivered by a PaaS provider makes it unnecessary for the user to rely on additional and/or specific hardware or software at internal level.

A full-fledged transition to a thoroughly public cloud system would appear not to be feasible in the short term on account of several reasons, in particular as regards large-sized entities like major companies or organizations that have to fulfil specific obligations – e.g. major banks, governmental bodies, large municipalities, etc. This can be accounted for mainly on two grounds: firstly, there is a momentum-like factor related to the investments required to achieve such transition; secondly, one has to take account of the especially valuable and/or sensitive information that is to be processed in the specific cases.

Another factor militating in favour of the reliance on private clouds (at least in the cases mentioned above) has to do with the circumstance that no public cloud provider can often ensure a quality of service (as based on SLAs, Service Level Agreements) such as to keep pace with the critical nature of the service the controller is to provide – maybe because bandwidth and reliability of the Net are not enough or appropriate in a given area, or else with regard to specific user-provider connections. On the other hand, one can reasonably assume that private clouds may be leased or rented in some of the above cases (because this may prove more cost-effective), or else hybrid cloud models (including both public and private components) can be deployed. The relevant implications would have to be considered carefully in all cases.

In the absence of internationally agreed standards, there is the risk of "do-it-yourself" cloud solutions, or else federated cloud solutions, which would entail increased lock-in dangers (as well as what have been termed "privacy monocultures")[51] and prevent full control over the data without ensuring interoperability. Both interoperability and data portability are indeed key factors for the development of cloud-based technology as well as in order to enable full exercise of the data protection rights vested in data subjects (such as access or rectification).

[51] See the European Parliament's study "Does it Help or Hinder? Promotion of Innovation on the Internet and Citizens' Right to Privacy" published in December 2011.

From this standpoint, the current debate over cloud technologies provides a significant example of the tension existing between cost-oriented and rights-oriented approaches, as briefly outlined in Section 2 above. Whilst relying on private clouds may be feasible and indeed advisable in a data protection perspective by having regard to the specific circumstances of the processing, this may not be viable to organisations in the long run mainly in a cost-oriented perspective. A careful assessment of the interests at stake is necessary, as no one-size-fits-all solution can be currently pointed to in this area.