GÖTEBORGS UNIVERSITET

Personuppgifter i molnet – nya regler, nya krav

En studie om offentliga verksamheters arbete med personuppgifter i molnet

Personal data within the cloud - new rules, new demands

A study about public organizations work with personal data in the cloud

Fredrik. Edlund
Robert. Nahra

Kandidatuppsats i informatik
Rapport nr. 2016:017

Göteborgs universitet
Institutionen för tillämpad informationsteknologi
Göteborg, Sverige, maj 2016

Abstrakt
Den senaste tidens händelser såsom Snowden's avslöjande om NSA's spioneri och Europas annullering av Safe Harbor-avtalet har lett till att ett nytt dataskyddsdirektiv tagits fram. Europa anser att det tidigare direktivet från 1995 föråldrats i takt med den tekniska utvecklingen. En teknik som kommit att påverka mycket är molntjänster. År 2014 gick 81 % av världens datatrafik genom molnet. EU har nyligen presenterat en ny förordning vid namn General Data Protection Regulation (GDPR). Syftet med förordningen är att skapa ett gemensamt regelverk för hur hantering av personuppgifter inom EU ska gå till. Studiens fokus är att undersöka vilka viktiga som är viktiga för offentliga verksamheter att beakta i och med övergången till den nya förordningen GDPR.

För att undersöka problemområdet har vi intervjuat tre offentliga verksamheter samt två välinsatta entiteter gällande GDPR. De huvudsakliga faktorer som framkommer i studien är: Den administrativa boten, incidentrapporteringen, dataskyddsombudsrollen samt registret.

Rapporten är skriven på svenska.

Nyckelord: Molntjänster, GDPR, PuL, förordning, EU, offentliga verksamheter.

Abstrakt
Recent events, such as the leaks of Snowden's documents about NSA’s spying and Europe’s dismissal of the Safe Harbor agreement has led to Europe rethinking their data protection directive. The main reason behind the change is that Europe believes that the previous directive from 1995 has expired in pace with recent technological developments. Cloud computing represents one of the technologies and was responsible for the transmission of 81 % of the world's data in 2014.

Europe has introduced a new Data protection act called General Data Protection Regulation (GDPR) with the purpose to create a common framework for the handling of personal data inside EU's borders. This study aims to identify imporant factors that the public sector should take into consideration with regards to the start of the new regulation GDPR. To manage this we’ve gone out and interviewed three organizations from the public sector and two legal knowing entities. The key factors that are shown in the study are: The new administrative fine, the incidentreporting, the data-protection role and the new registry.

The report is written in Swedish

Keywords: Cloud computing, GDPR, PuL, regulation, EU, public sector.

TACK

Tack till vår kontaktperson på Atea, Daniel Back som hjälpt och inspirerat oss att skriva om GDPR och molntjänster. Tack även till Olov Alderholm, och Alf Holmberg på Atea för kontinuerlig feedback under arbetets gång.

Tack alla informanter på offentliga verksamheter för att ni ställde upp på intervjuer.

Tack Albin Westerlund som underlättade litteratursökningen i studien.

Slutligen stort tack till vår handledare Aida Hazdic som under arbetets gång hjälpt och inspirerat oss och gett feedback regelbundet.

Innehåll

1. Inledning

Cloud computing eller molntjänster representerar en av dagens mest omtalade teknologier. 2014 gick 81 % av hela världens mobila datatrafik genom molnet (Columbus 2014). Molntjänster möjliggör för företag att erbjuda produkter som en tjänst som hyrs via internet istället för färdiga produkter som behöver köpas (Greenwood, Khajeh-Hosseini, Smith, & Sommerville 2011). National Institutes of Standards and Technology (NIST) definierar molntjänster som en teknologi där du enkelt kan komma åt IT-resurser såsom t.ex nätverk, servers, lagring och applikationer. Resurserna kan därefter enkelt användas utan att interaktion med den som erbjuder tjänsten krävs (NIST 2011).

Då mängden information som går igenom molnet växer har tekniken på senare år associerats till många säkerhetsrisker. Det har lett till att tilliten till molntjänster minskat drastiskt på senare tid (Stenvall, 2014). I media har dataintrång och större skandaler inom EU uppmärksammats i relation till molntjänster. (Holmström 2013; Rensfeldt 2013). Problemet ligger både i den tekniska aspekten av molnet, men även i den bristande regleringen. Idag är det inte alltid självklart vem det är som har ansvar för de personuppgifter som lagras i molnet, eller hur man bör gå tillväga vid felhantering av informationen (Fernandes, Soares, Gomes, Freire & Inácio 2013). Trots detta delas och samlas alltmer information online (European Commission 2012).

Vidare kan informationen som lagras i molnet ha en varierande geografisk plats, vilket skapar legala problem då olika lagar gäller för olika länder (Karlsson 2014). Ytterligare komplikationer skapas när organisationer inte heller har någon obligation att rapportera de dataförluster som rör personuppgifter till en högre instans. Avsaknad av information om hur ofta eller varför förlust av personuppgifter sker är därför vanligt (European Commission 2012; Delphi 2016).

För att förbättra säkerhetsarbetet vid personuppgiftshantering har EU beslutat att införa en ny dataskyddsförordning vars syfte är att skapa ett gemensamt regelverk för hur verksamheter ska hantera personuppgifter. Förordningen avser främst att gälla medlemsländerna i Europa, men kommer att påverka alla länder som hanterar personuppgifter inom EU (Europeiska Kommissionen 2012,2015).
General Data Protection Regulation eller (GDPR) som förodningen benämnts kommer att ersätta Personuppgiftslagen (PuL) som för nuvarande gäller i Sverige. Förordningen leder till ny problematik och förändringar som främst påverkar verksamheter som behandlar personuppgifter då de kommer behöva anpassa sin verksamhet till de nya bestämmelserna. Vidare kan verksamheter som felbehandlar personuppgifter komma att bötfällas när GDPR träder i kraft (Datainspektionen 2016a).

Tidigare studier om molntjänster med fokus på säkerheten är inte svåra att komma över (Naser, Kamil & Thomas 2015; Kazim & Zhu 2015; Lee 2012; NIST 2011). Molntjänster är som nämnts tidigare en teknik som fått mycket uppmärksamhet de senaste åren. Dock är det svårt att finna studier som behandlar molntjänster i samband med personuppgifter. Den forskning som finns idag om hantering av personuppgifter kommer även inom kort att bli mindre aktuell då GDPR träder i kraft.

Allt fler offentliga verksamheter tar steget ut i molnet, vilket påverkar deras hantering av personuppgifter (Tieto 2016; Datainspektionen 2016a; ComputerSweden 2013). Europeiska Komissionen (2015) och Delphi (2016) beskriver hur GDPR kommer ställa nya krav på verksamheter som behandlar personuppgifter vilket gör det till ett intressant problemområde att studera.

1.1 Syfte och frågeställning

Vår uppsats ämnar att undersöka viktiga faktorer som offentliga verksamheter behöver ha i åtanke i och med övergången till den nya förordningen GDPR. Motivet är att identifiera vad offentliga verksamheter i Sverige borde tänka på vid hantering av personuppgifter i molnet.

Utifrån ovanstående information är studiens frågeställning följande:

"Vilka faktorer är viktiga för offentliga verksamheter att beakta i och med övergången till den nya förordningen GDPR?"

Studien anses relevant då den undersöker en förordning som kommer att påverka offentliga verksamheters hantering av personuppgifter i molnet. När GDPR träder i kraft kommer även samtliga verksamheter inom EU att behöva följa de nya bestämmelserna. Det här innebär att studien anses intressant för alla verksamheter eller statliga organisationer som behandlar personuppgifter.

1.2 Definition av begrepp

För att upprätthålla tydlighet i studien när vi talar om tekniken har vi valt att använda oss av det svenska begreppet molntjänster eller molnet och utgått från NIST definition av vad tekniken innebär (se 1).

När vi i denna uppsats diskuterar reglering av information i molnet är det viktigt att skilja på begreppen direktiv och förordning. Ett direktiv är när medlemsländerna inom EU tar fram gemensamma mål som medlemsländerna själva får bestämma hur de vill uppnå. Detta kan exempelvis göras genom att stifta egna nationella lagar. En förordning är däremot en bindande rättsakt som alla EU-länder ska tillämpa i sin helhet. Alltså gäller samma lagar för alla medlemsländer om det är en förordning (Europeiska Unionen u.å.).

När vi talar om personuppgifter menar vi all information som direkt eller indirekt kan kopplas till en fysisk person. En personuppgift kan vara allting från en bild till en IP-adress (Delphi 2016).

1.3 Avgränsning

GDPR är en förordning och står för "General Data Protection Regulation". Förordningen omfattar en mängd olika områden. Vi har i studien därför valt att fokusera på hur offentliga verksamheter som behandlar personuppgifter i molnet påverkas av de nya bestämmelserna.

Vi har även valt att endast fokusera på offentliga verksamheter i Sverige som har eller ska införskaffa molntjänster. Detta för att kunna identifiera faktorer som är viktiga för verksamheterna att tänka på i och med övergången till GDPR.

1.4 Disposition

I nästkommande avsnitt presenteras en bakgrund som förväntas ge insikter om tidigare regleringar relaterade till personuppgifter och den nya förordningen. Därefter presenteras teorin där viktiga aspekter för problemområdet förklaras. Studiens utredningsmetodik, tillvägagångssätt och genomförande beskrivs i kapitel 3 metod. Resultaten av datainsamlingen presenteras sedan i kapitel 4. Slutligen presenteras studiens diskussion och slutsats i kapitel 5 och 6.

1.5 Bakgrund till studien

Personuppgiftslagen (PuL) trädde i kraft år 1998 som en följd av EUs dataskyddsdirektiv som fastslogs samma år.
Syftet med PuL är att skydda människors personuppgifter, samtidigt som man inte kränker en persons integritet vid behandling av dessa uppgifter (Datainspektionen u.å.d). Lagen behandlar grundläggande krav för att personuppgifter ska fås samlas in, hur länge personuppgifterna får sparas, samt hur lagring och hantering av personuppgifterna ska gå till.
PuL gäller för alla företag, myndigheter och organisationer med få undantag (Datainspektionen u.å.d).

I verksamheter som behandlar personuppgifter måste alltid en eller flera personuppgiftsansvariga utses. En personuppgiftsansvarig har som uppgift att självständigt ansvara för att personuppgiftslagen uppfylls för verksamheten personen arbetar för. Uppfylls inte personuppgiftsansvaret gentemot en registrerad har den registrerade rätten till att begära skadestånd av verksamheten (Delphi 2016; Datainspektionen u.å.d). I de fall av att en verksamhet som behandlar personuppgifter outsourcat sin data till exempelvis en molntjänstleverantör, måste ett så kallat personuppgiftsbiträde utses. Biträdets uppgift är att behandla personuppgifter för den personuppgiftsansvarige i verksamheten. Viktigt att notera är att det fortfarande är verksamheten och den personuppgiftsansvarige som har ansvar för datat och inte molntjänstleverantören eller personuppgiftsbiträdet (Delphi 2016).

I Sverige är det tillsynsmyndigheten Datainspektionen som ser till att personuppgiftslagen följs.
Datainspektionens är en myndighet vars uppgift är att bidra till att behandlingen av personuppgifter sker på ett lagligt och icke kränkande sett. Som tillsynsmyndighet arbetar datainspektionen både med att understödja verksamheter med information om vilka lagar och regler som gäller, samt se till att det faktiskt följs (Datainspektionen u.å.e).

För att bättre förstå varför EU valt att påbörja införandet av General Data Protection Regulation (GDPR) är det viktigt att förstå tidigare händelser som har lett fram till beslutet.
Den 24 oktober 1995 antogs Europaparlamentets och rådets direktiv 95/46/EG, L 281, 23.11.1995, ss. 0031 – 0050 vars syfte var att skapa ett ramverk för hur skydd av enskilda personer avseende behandling av personuppgifter och om det fria flödet av sådana uppgifter.
Direktivets syfte beskrivs under artikel 2 **"**Definitioner**"** i två punkter som lyder: 1.**"**Medlemsstaterna skall i enlighet med detta direktiv skydda fysiska personers grundläggande fri- och rättigheter, särskilt rätten till privatliv, i samband med behandling av personuppgifter**"**. 2. **"**Medlemsstaterna får varken begränsa eller förbjuda det fria flödet av personuppgifter mellan medlemsstaterna av skäl som har samband med det under punkt 1 föreskrivna skyddet.**"**

En annan lag som varit en viktig del i den historiska utvecklingen är Safe Harbor avtalet som slöts mellan Europa och USA år 2000. Anledningarna till att avtalet slöts är många, men en specifikt viktig händelse går att finna. I och med införandet av dataskyddsdirektivet år 1995, beskriver Long och Quek (2002) hur USA inte längre uppfyllde Europas nya krav på hantering av personuppgifter.
USA hade två val, antingen riskera att EU inte längre tillät information om Europeiska medborgare att skickas till USA, eller att anpassa lagen till att uppfylla EU's nya krav på personuppgiftshantering. Utfallet blev Safe Harbor avtalet (Long & Quek 2002).
Safe Harbor avtalet blev dock nyligen annullerat. Den 6 oktober 2015 klubbades ett fall i Europas högsta domstol igenom som ogiltigförklarade avtalet (Winston & Strawn 2015). I fallet "Schrems v. Data Protection Commissioner" argumenterade en Österrikisk medborgare vid namn Max Schrems för att Facebook Irland inte borde få skicka personuppgifter om honom till USA. Detta med anledning av att Edward Snowdens tidigare läckor påvisade att National Security Agency (NSA) spionerade på allmänheten för den amerikanska regeringens räkning (Winston & Strawn 2015; International Bussiness Times 2015).

2015 gick EU ut med ett pressmeddelande. I pressmeddelandet beskrivs bland annat att européer är oroliga över hur deras personuppgifter hanteras på nätet (Europeiska Kommissionen 2015).
Med tanke på Edward Snowdens uppmärksammade fall och Europadomstolens ogiltighetsförklaring av Safe Harbor, har EU diskuterat och tagit fram en ny förordning för hur hantering av personuppgifter bör gå till (Datainspektionen 2016a, b). Den nya förordningen vid namn GDPR kommer att internationellt ersätta det gamla direktivet och nationellt användas istället för PuL.
Till skillnad från dataskyddsdirektiven från 1995 är GDPR en förordning vilket innebär att alla EU länder måste tillämpa lagen i sin helhet. Syftet med lagen är att skapa ett bättre integritetsskydd för individer och underlätta för överföringen av personuppgifter inom EU (Delphi 2016; Datainspektionen 2016a; Europeiska Kommissionen 2012, 2015). Främst kommer överföringen av personuppgifter att regleras för att underlätta granskning om vilken information som sparas, vem informationen tillhör samt hur länge informationen kommer att existera (Delphi 2016; Datainspektionen 2016a; Europeiska Kommissionen 2012; Europeiska Kommissionen 2015).
Vidare kommer alla länder som behandlar personuppgifter från EU oavsett geografisk plats behöva följa GDPR. Bevekelsegrunden är att öka tillsynen för vilka länder som är tillåtna att ta emot personuppgifter ifrån EU. GDPR kommer även ställa ett obligatoriskt krav på samtliga medlemsländer till att inrätta en tillsynsmyndighet. Tillsynsmyndigheten ska fungera som en svarsperson för rättsliga fall om personuppgifter. Samtliga verksamheter som behandlar personuppgifter kommer ha en skyldighet att rapportera in förlust av personuppgifter till tillsynsmyndigheten (Delphi 2016; Datainspektionen 2016a).

GDPR fastslår även att verksamheter kommer behöva ge ut information om hur länge personuppgifter lagras och vad för typ av information det rör sig om. Informationen om personuppgifter som lagras ska vara beskrivet på ett begripligt sätt och vara enkelt att komma åt (Delphi 2016). Alla verksamheter kommer vara tvungna att inrätta ett dataskyddsombud, vilket kommer att vara en anställd på verksamheten eller alternativt en konsult som ansvarar för personuppgiftshantering (Delphi 2016). Dataskyddsombudets uppgift är att bidra med expertkunnande om lagstiftning och praxis till verksamheten (Delphi 2016). Det ska även upprättas ett register som dataskyddsombudet ansvarar för. Registret ska tydligt förklara hur verksamheten använder personuppgifter och ska kunna redovisas för en tillsynsmyndighet vid begäran (Delphi 2016; Datainspektionen 2016a).

Avslutningsvis kommer GDPR att införa administrativa böter för verksamheter som missbrukar hanteringen av personuppgifter. Hur kraftiga böter beror på vilka säkerhetsåtgärder som vidtagits, vilken information som läckt ut, samt om verksamheten samarbetat med tillsynsmyndigheten och gjort en anmälan av händelsen. Botens storlek varierar mellan 2-4% av en koncerns globala omsättning med en maxgräns på 20 miljoner euro (Delphi 2016; Datainspektionen 2016). Förordningen kommer att träda i kraft 2018 och förväntas vara fullt fungerande 2020.

2. Teori

Följande kapitel ämnar att ge en förståelse för offentliga verksamheter och deras problematik med personuppgifter i molnet. Avsnittet inleds med en förklaring av offentliga verksamheters användning av IT och molntjänster. Därefter presenteras den reglering som påverkar molntjänster och personuppgiftshantering för att ge en bättre förståelse för det studerade området.

2.1 Offentliga verksamheter och molntjänster

Offentliga verksamheter är en del av den offentliga sektorn och består av verksamheter som finansieras av allmänna medel. Vård och omsorg, utbildning, kollektivtrafik samt infrastruktur är exempel på verksamheter som ligger inom den offentliga sektorn i Sverige (Libell 2013)

Det har blivit allt vanligare att offentliga verksamheter använder sig av IT (IFI 2010; Libell 2013).
IT står för informationsteknologi och är ett samlingsbegrepp för tekniska möjligheter som skapas med hjälp av datorteknik (Nationalencyklopedin 2016). Idag använder cirka 94 % av Sveriges befolkning Internet (Post och Telestyrelsen 2015). Det har medfört att användningen av IT inom offentliga verksamheter ökat på senare år. Den totala kostnaden för offentliga verksamheters användning av IT uppgick 2010 till cirka 10 miljarder kronor (IFI 2010; Libell 2013).
Genom att utnyttja IT kan offentliga verksamheter erbjuda sina tjänster elektroniskt via vad som kallas för e-tjänster (SKL 2014). På senare tid har offentliga verksamheter börjat erbjuda dessa elektroniska tjänster med hjälp av molntjänster (Tieto 2016; Datainspektionen u.å.c). Det här beror på att det finns många fördelar för verksamheterna med att använda sig av tekniken.
En fördel är att verksamheterna kan ta del av en tjänst eller produkt via Internet istället för att äga den själva (Greenwood et al. 2011). Ett exempel på hur molntjänsterna kan hyras in är via SaaS “Software as a Service” (Dubey & Wagle 2007).

En annan fördel är att de offentliga verksamheterna kan förflytta hela eller stora delar av sina interna verksamhetsprocesser till en eller flera externa leverantörer. Leverantören tar sedan över administrationen av aktiviteterna enligt vad som avtalas (Subhankhar 2012). Yttligare fördelar med molntjänster är att verksamheter enkelt kan skala upp eller ned sin verksamhets användning av det som outsourcas beroende på behov (Marston, Li, Bandypadhyay & Ghalsasi 2011). Att använda sig av 1000 servers för en timme kostar inte mer än att använda sig av en enskild server i 1000 timmar (Armbrust et al. 2010). Atkinson och Meager (1986) beskriver att organisationer väljer vad som kan outsourcas genom att skilja på processer som är viktiga för verksamheten, och processer som är av simplare karaktär (Se Riley & Tamkin 1996 s.11). Anledningen till att offentliga verksamheter använder sig av molntjänster är oftast att spara verksamheten pengar (Corbett 2004). Naser (2015) beskriver även att verksamheter i vissa fall kan uppnå större säkerhet än tidigare med hjälp av molntjänster. NIST (2011) menar

däremot att verksamheter behöver finna en balans mellan säkerheten som krävs för att molntjänsten ska fungera, gentemot vilken ekonomiska nytta som användningen av molnet leder till.

2.2 Reglering av information i molnet

Offentliga verksamheter har ett antal lagar och regler som behöver följas gällande hantering av personuppgifter. Som tidigare beskrivs (se 1.5) är i dagsläget personuppgiftslagen (PuL) den rådande lagen. Till skillnad från det traditionella sättet att hantera alla verksamhetsprocesser inhouse (internt) lämnar verksamheter vid införskaffandet av molntjänster över delar av sina verksamhetsprocesser till molntjänstleverantören. För offentliga verksamheter som behandlar personuppgifter uppstår därför legala problem då de inte längre har full kontroll över sin information (Karlsson 2014; Datainspektionen u.å.c). Detta beror på att tekniken molntjänster är designad på så sätt att molntjänstleverantörens servrar kan befinna sig i olika länder. Informationen kan därför förflyttas mellan olika landsgränser vilket leder till att det är svårt att avgöra vart informationen befinner sig (Karlsson 2014). Detta leder till att konflikter mellan olika länders dataskyddslagstiftningar uppstå då olika länder har olika lagstiftningar som reglerar hanteringen av personuppgifter (Karlsson 2014).

Med koppling till den ovanstående problematiken med molntjänster beskriver NIST (2011), Brodkin (2008), Datainspektionen (u.å.c) och Karlsson (2014) att många molntjänstleverantörer använder sig av standardavtal. Det är därför intressant för verksamheter att omförhandla avtalen så att de uppfyller lagkraven som ställs för den geografiska plats de befinner sig på (NIST 2011; Brodkin 2008; Datainspektionen u.å.c; Karlsson 2014). För en offentlig verksamhet i Sverige som behandlar personuppgifter kan det till exempel handla om att molntjänstavtalet behöver omarbetas för att uppfylla PuL.

Vidare talar Datainspektionen (u.å.c) om en ytterligare aspekt offentliga verksamheter bör ta i beaktning vid införskaffande av molntjänster. Trots att molntjänstleverantören behandlar personuppgifterna åt verksamheten är det fortfarande verksamheten som har ansvaret för personuppgifterna. Detta kallas för att man är personuppgiftsansvarig (se 1.5). Den personuppgiftsansvarige måste även utföra en risk- och sårbarhetsanalys vid införskaffandet av molntjänster för att avgöra om den valda molntjänstleverantören uppfyller de kriterier som krävs för att behandla personuppgifter. Syftet med en risk och sårbarhetsanalys är att öka myndigheters uppfattning om hot, risker och sårbarheter inom verkningsområdet, samt ta fram en plan för hur dessa kan motverkas (MSB 2015; MSB 2011)

Förordningen General Data Protection Regulation (GDPR) har som syfte att tackla ovanstående problematik genom att skapa en gemensam dataskyddsförordning. Detta betyder i praktiken att alla Europeiska medlemsländer då kommer behandla personuppgifter exakt likadant oberoende på geografisk plats (se 1.5).

3. Metod

3.1 Kvalitativ metod

För att besvara forskningsfrågan **"***Vilka faktorer är viktiga för offentliga verksamheter att beakta i och med övergången till den nya förordningen GDPR?"* valde vi att använda oss av en kvalitativ forskningsmetodik med ett deskriptivt förhållningssätt. Vi valde denna kvalitativa metod för att på djupet kunna studera problemområdet. Samtidigt ville vi jämföra informanternas uppfattning om hur personuppgifter behandlas i molnet samt hur detta kommer påverkas av GDPR. Att arbeta deskriptivt innebär att man beskriver hur någonting är, istället för att tala om hur någonting bör vara (Shield & Rangarajan 2013).

På grund av studiens komplexitet var vi först tvungna att skapa oss en uppfattning om GDPR. Utgångspunkten har därför varit att arbeta deduktivt med teorierna som grund. Att arbeta deduktivt innebär att teorin testas mot verkligheten, till skillnad från induktion där man skapar sin teori utifrån observationer av verkligheten (Leduc 2007a). Efter genomförda intervjuer valde vi att komplettera teorin då vi i början av studien inte besatt tillräckligt mycket information om ämnet. Det här innebär att vi först använde oss av deduktion för att sedan induktivt bygga vidare på teorin.

Vidare fastställdes, behandlades och analyserades det insamlade materialet för att uppnå en bredare förståelse för det fenomen som studerades (Patel & Davidsson 2011). Utifrån kvalitativa metoder har vi utgått från användning av dokumentanalys samt semistrukturerade intervjuer. Under arbetets gång har dock kvalitativa intervjuer varit den främsta informationskällan. Detta för att det inte går att återfinna mycket vetenskapliga publikationer som diskuterar området. Åsberg (2001) nämner att användandet av olika typer av metoder är vanligt vid datainsamling när man talar om kvalitativ forskning. Dessutom kompletterade metoderna varandra och gav oss en förbättrad förståelse av problemområdet.

Patel och Davidsson (2011) beskriver att intervjuer som är semistrukturerade oftast är väldigt flexibla och att frågorna i dessa intervjuer håller låg standardisering. Det här har lett till att vi själva har kunnat variera frågorna till att vara både öppna och ostrukturerade eller precisa och mer strukturerade beroende på om vi önskade ett specifikt kort svar eller ett öppet och mer utförligt svar. Patel och Davidsson (2011) menar även att för att lyckas med en intervju, behöver intervjuaren hjälpa intervjupersonen bygga upp ett meningsfullt och sammanhängande resonemang om det studerade fenomenet. Intervjufrågorna ställdes därför i ordning där vi inledningsvis talade allmänt om ämnet för att senare diskutera mer specifika frågor. Vi undvek även att ställa frågor som riskerade att bli besvarade med ett ja eller nej.

För att få en grundlig förståelse över det studerade området har vi även utgått ifrån dokumentanalys. Dokumentanalys är att studera redan tillgängligt material relaterat till problemområdet eller om problemområdet (Patel & Davidsson 2011). Patel och Davidsson (2011) nämner att det är viktigt att försöka fastställa att de dokument som presenteras och används i dokumentanalysen är sannolika. Det här har kontrollerats genom att vi bekräftat informationen i diverse källor för att försäkra oss om att den stämmer. Dessutom är majoriteten av informationen som använts för att diskutera lagar och regler hämtad från nationella och internationella organ vilket i sig självt skapar legitimitet. Dokumenten som presenterar information om de risker som molntjänster medför anser vi också som sannolika. Anledningen är att informationen har tagits från respekterade tidningar och tidsskrifter som har flera artiklar där ämnet behandlats.

3.2 Datainsamling

Med avsikt att finna ett intressant problemområde att studera genomfördes först en förstudie hos Atea som resulterade i forskningsfrågan. Atea är en av europas största cloudintegratörer och specialister inom IT-infrastruktur. Efter förstudien genomfördes fem intervjuer under en period på fyra veckor på varierande platser i Göteborg. Vi träffade antingen informanterna fysiskt, eller talade via kommunikationsmedlet skype. De tillfällen skypeintervjuer genomfördes berodde främst på att personen som skulle intervjuas ansåg att tiden inte fanns för att planera in ett fysiskt möte, eller att distansen mellan oss var för lång. Fortsättningsvis spelade vi dessutom in och transkriberade eller antecknade varje intervju. Detta för att enklare kunna analysera resultatet. På begäran av en av informanterna skickade vi även ut frågorna i förväg. Detta gjordes sedan till samtliga informanter för att det skulle vara lika för alla.

Gällande frågorna har vi utgått från tre olika teman som använts i intervjuerna för att kunna besvara forskningsfrågan. De tre teman som togs fram var molntjänster, lagar och regler samt risk-och sårbarhetsanalys. Risk- och sårbarhetsanalys bakades dock in i temat lagar och regler eftersom vi ansåg att temat inte var tillräckligt omfattande för att kunna skrivas enskilt efter att intervjuerna genomförts. Vi avsåg även att få en bredare förståelse för problemområdet och valde därför att intervjua högt uppsatta personer inom olika verksamheter. I intervjuerna går det därför att återfinna IT-chefer, säkerhetsspecialister, informationssäkerhetschefer samt en försäljningschef.

Samtliga informanter informerades om att det insamlade materialet kommer att användas i studien samt att namnet på deras organisation kan komma att synas. Tiden det tog att genomföra en intervju varierade beroende på om den ägde rum fysiskt, via telefon eller skype men hölls alltid inom en tidsram på 20-60 minuter. Under intervjuerna presenterade vi först oss själva, för att kort därefter få en introduktion av intervjupersonen och dennes roll i sin verksamhet. Därefter arbetade vi oss igenom de tre teman molntjänster, lagar och regler samt risk- och sårbarhetsanalys som tagits fram samt ställde följdfrågor när vi kände att någonting saknades eller kunde adderas. I övrigt upplevde vi inte att någon av frågorna som ställdes var för svåra för informanterna att svara på och fick intrycket att de alla var intresserade av ämnet.

3.3 Analysmetod

Tematisk analys är en metod som sällan uppmärksammas, men som erbjuder ett enkelt sätt för att analysera kvalitativ data (Braun & Clarke 2006). Analysen bygger på att ta fram relevanta teman för studien och därefter transkribera materialet utefter det. I studien har vi använt metoden för att ta fram tre teman och därigenom skapa en tydlighet i presentationen av det empiriska resultatet. Vidare har vi även ställt teorin mot kategoriseringen och de rubriksättningarna som vi har valt. Trots detta har dock inte alla teman använts för varje intervju. Braun och Clarke (2006) menar att eftersom det handlar om kvalitativ analys, finns det inget som säger hur stor del av informationen som behöver representera ett visst tema för att den ska kunna anses vara ett tema. Fördelen med att använda sig av en tematisk analys har i vår studie varit att vi iterativt kunnat fokusera på de områden som ansågs vara viktiga för studien (Braun & Clarke 2006).

3.4 Studiens relevans och överförbarhet

För att kunna granska och dra slutsatser från den använda metoden är det viktigt att begreppen reliabilitet och validitet diskuteras. Med validitet menas mätinstrumentets förmåga att mäta det som det påstås mäta. Reliabilitet handlar istället om mätmetoden skulle ge samma resultat vid upprepade mätningar och är okänslig för slumpens inverkan (Leduc 2007b).
Under studiens gång har avsikten varit att använda tematisering för att behandla tre olika teman. Detta för att validera studiens utfall och öka reliabiliteten vid liknande studier. Nackdelarna med att använda sig av tematisering är inte metoden i sig, utan istället att den är beroende av väl genomförda analyser samt passande intervjufrågor (Braun & Clarke 2006). Genom att säkerställa intervjupersonernas roll och erfarenhet inom sitt område har vi lyckats undvika att ställa frågor där intervjupersonen inte haft något svar på frågan på grund av icke tillräcklig kunskap. Dessutom har varje intervju transkriberats direkt efter intervjutillfället. Leduc (2007b) menar att det här bör göras för att uppnå samtidig validitet.

Vidare är tematisering en flexibel metod som tillåter analysen av materialet att genomföras på många olika sätt. Även om det här kan uppfattas som positivt innebär det att det kan vara svårt att bestämma sig för vilken aspekt av datan som man vill fokusera på (Braun & Clarke 2006). Det här går att se i vårt resultat där vi har sammanställt informationen från informanterna som kommer att presenteras i nästa stycke.

Studiens validitet kan även styrkas av att vi har använt sekundärkällor för att säkerställa att informationen som använts är legitim (Leduc 2007b). En problematik som vi stötte på under dokumentanalysen var dock svårigheten i att finna information om GDPR. Vi fick därför leta i officiella EU dokument, eller kontakta personer som arbetade med utbildningar inom ämnet för att kunna genomföra studien. Däremot anser vi att det här endast har lett till en ökat tillförlitlighet för de dokument som använts.

3.5 Presentation av urvalsgruppen

För att säkerhetsställa att intervjuerna som genomfördes var relevanta för studien kontrollerades att de offentliga verksamheter som undersöktes infört, eller påbörjat införandet av molntjänster. Patel och Davidsson (2011) beskriver att en kvalitativ studie kan utföras på olika sätt och att man bör anpassa metoden efter situationen. Med tanke på studiens begränsade tidsram och den omfattande dokumentanalysen anser vi att fem intervjuer var tillräckligt för studien.

Valet av urvalspersoner gjordes utifrån ett par kriterier som sattes upp. För att få en bra förståelse för vilka faktorer som är viktiga för offentliga verksamheter att beakta i och med övergången till GDPR innebar det första kriteriet att minst två av informanterna skulle vara väl insatta inom området. Därför genomfördes den första intervjun med en väl insatt person inom GPDR och molntjänster. Att lokalisera den andra informanten var simpelt då en väldigt uppenbar lösning var att kontakta den myndighet i Sverige som administrerar personuppgiftshantering. Det här resulterade i att vår andra intervjuperson arbetade på Datainspektionen. Valet av att inte anonymisera de två expertutlåtandena baseras på att det är relevant för studien att kunna visa vilka verksamheter vi har talat med. Vi ville även påvisa att expertutlåtandena kommer ifrån olika verksamheter som på olika sätt har en koppling till studiens problemområde.

Målet var sedan att intervjua representanter från tre offentliga verksamheter inom olika områden. En kommun, ett statligt organ samt någon inom sjukvården. Det utmynnade istället i två kommuner och ett statligt verk. Anledningen var att det var svårt att finna någon inom

sjukvården som arbetade med molntjänster. Därefter kom vi fram till att sjukvården präglas av egna lagar som påverkar personuppgiftshantering. Detta hade skapat en konflikt med studiens avgränsning och fått studien att hamna utanför sitt scope. Vi har däremot valt att anonymisera de offentliga verksamheterna på grund av att det inte är relevant för studien vilken, eller vilka kommuner och statliga verk vi har talat med.

Informant	Roll	Intervjumetod	Längd (min)
1. Expert	IT & försäljningschef	Fysisk	52:42
2. Expert	IT-säkerhetsspecialist	Skype	27:32
3. Offentlig verksamhet	IT strateg & It chef	Fysisk	61:23
4. Offentlig verksamhet	Informationssäkerhetschef	Fysisk	43:14
5. Offentlig verksamhet	IT-chef	Skype	41:15

Figur 1: Tabell av informantgrupperna

4. Resultat

I följande avsnitt presenteras resultatet av undersökningen i form av att vi först presenterar de två experternas utlåtanden separat. Detta då frågor om både molntjänster och reglering ställdes till den första experten medan endast frågor om reglering ställdes till expert 2. Sedan presenteras de tre offentliga verksamheternas svar tillsammans för att enklare kunna identifiera skillnader eller likheter i deras svar. För att enklare åtskilja experterna och de offentliga verksamheternas svar i diskussionen har vi valt att namnge informant 1 respektive 2 som expert 1 och 2. Resultatet presenteras i de teman som tidigare tagits upp i studien (Molntjänster & Lagar och regler).

4.1 Informant 1 (Expert 1)

Molntjänster

Informant 1 beskrev Microsoft som dominerande på frågan om vilka molntjänster som de erbjuder idag med Microsoft Azure och office 365 som de ledande. "*Jag tror Amazon kommer vara en stor spelare på svenska marknaden i framtiden, det är de inte idag*".
Vidare diskuterades vilka utmaningar informanten ansåg präglade molntjänster.
Informanten ansåg att utmaningen handlar om att lägga ut rätt information i molnet. För att göra detta måste verksamheten kunna analysera vad för typ av information som hanteras i verksamheten. Informanten talade om att rollen som molnintegratör omfattar att hjälpa kunden med dessa frågor och analyser. "*Just den informationsbiten är den största utmaningen både för oss och för kunden*".

Därefter talade informanten om att kundens inställning till molnet inte förändras efter att tjänsten implementerats. "*När de väl beslutar sig för att gå ut i molnet har de redan gjort sitt beslut i att det känns bra*" Informanten nämnde även att det som stoppar eller fördröjer processen för offentliga verksamheter är legala frågor. Vad för information får vi lägga i molnet? Personuppgiftshanteringen? Hur säker är informationen? "*Det går nog inte att lägga information på ett fysiskt säkrare ställe än i de stora molnleverantörernas datacenter*".
Offentliga verksamheter är intresserade av frågor om var informationen faktiskt befinner sig och hur det fungerar med backups.
Andra aspekter som offentliga verksamheter behöver ha i åtanke är att de fortfarande är personuppgiftsansvariga när de väljer att lägga personuppgifter i molnet. **"***Det är mindre osäkra på hur datat ligger men mer osäkra på lagarna och förordningarna de har att förhålla sig till. Där ligger osäkerheten***"**.

Därefter talade vi om vem som idag bär ansvaret för datan om någonting händer och hur arbetsprocessen ser ut. Informanten beskrev att det idag inte råder någon gemensam struktur för rapporteringen av IT-incidenter. I dagsläget bör en polisanmälan göras vid förlust av personinformation. Det finns dock ingen skyldighet vilket innebär att vissa verksamheter gör en anmälan medan vissa andra inte gör det. Generellt beskrev informanten arbetsprocessen som *"Om man blir av med personuppgifter via IT-brottslighet så bör detta bli en polissak som skall anmälas. Nästa steg blir att isolera skadan och minimera effekten av förlusten. Därefter ska företaget/organisationen täppa till eventuella säkerhetshål".* Informanten beskrev dock att förordningen GDPR kommer att ändra på detta "*Framöver kommer det här se annorlunda ut då man kommer vara tvungen att anmäla dataintrång till Datainspektionen eller MSB, alternativt någon instans inom EU.*

Lagar och regler

Nästa Tema i intervjun avsåg att diskutera den nya förordningen GDPR. Inledningsvis frågade vi om GDPR kommer att öka tilliten till molnet. Informanten förklarade att det finns två viktiga aspekter i förordningen. Den ena är att GDPR förhoppningsvis skapar ett unisont tänkande kring informationssäkerhet för personuppgifter inom EU. Informanten beskrev att det i dagsläget uppstår mycket legala problem med molnet på grund av att olika dataskyddslagar gäller i olika länder. En av GDPRs funktioner är då tänkt att lösa det problemet. Den andra aspekten som beskrivs är att man i framtiden kommer vara tvungen att rapportera in informationsstöld och dataintrång av personuppgifter. I dagsläget finns inga krav på detta.

Vidare frågade vi informanten om outsourcing kommer att påverkas av att GDPR införs. Den största skillnaden beskrevs av informanten att vara hur kunden själv ska kunna upptäcka dataintrång eller informationsförlust "*Kan du idag kontrollera att du har blivit av med personuppgifter? Om jag sitter på företaget och mailar hela användardatabasen med personnummer, inkomstuppgifter och allt, har verksamheten koll på det? Nej kommer nog många att svara".* Att skapa loggar och arbetsrutiner för hur denna typ av information bör hanteras är ett av de största problemen för många verksamheter i dagsläget beskrev informanten.

Därefter frågade vi om informanten ansåg att det råder brister eller en icke tillräcklig reglering i förordningen GDPR.

Svaret blev att som informanten ser på GDPR för tillfället så är den vältäckande. Informanten beskrev att hen hade velat se en ännu hårdare lag. Så som GDPR ser ut idag handlar det om dataintrång och anmälan gällande personuppgifter. Det hade varit mer intressant enligt informanten om det hade gällt allmänt för IT-incidenter och inte bara för personuppgifter. *"Men i övrigt tycker jag att GDPR känns ganska välgenomtänkt, ungefär som PuL"* avslutar informanten med.

Vidare diskuterades hur informanten tror att förändringen med hur personuppgifter ska hanteras vid införandet av GDPR kommer att påverka verksamheter i Sverige. Svaret blev att GDPR börjar gälla i början av 2018, med två års "smekperiod" från april 2016.*"Förhoppningen är att verksamheter blir mer rädda om deras personuppgifter samtidigt som anmälningarna ökar så att man får en rättvis bild av vad som händer på marknaden"*. Informanten beskrev även att förordningen kommer resultera i striktare reglering om hur personuppgifter får färdas, detta för att förebygga mindre trevliga utfall av felhantering.

En fråga ställdes om vem informanten anser har en central roll i arbetet med GDPR utifrån ett nationellt perspektiv. Informanten beskrev hur SKL (Sveriges Kommuner och Landsting), Datainspektionen, MSB (Myndigheten för samhällsskydd och beredskap) samt Polisen alla har en viktig roll att spela. Informanten hoppas att ansvarigt organ inom EU kommer ha tillräckligt med resurser till förfogan för att se till att GDPR verkligen följs.

Vi talade vidare med informanten om dennes tankar kring den bot som kan komma att utfärdas vid misslyckande av att rapportera in detaljer kring försvunna eller felhanterade personuppgifter. Boten beskrevs vara intressant och viktig för verksamheterna att tänka på. Informanten svarade: *"Det som diskuteras är 4 % av den globala årsomsättningen, dock högst 20 miljoner euro, vilket är en hel del summa pengar.".* Informanten förklarade vidare att dessa böter då kommer gälla vid en verksamets misslyckande av att rapportera stöld eller felhantering av personuppgifter inom 72 timmar från att det upptäckts. Informanten tror att boten finns till för avskräckande syfte och hoppas att verksamheter inte korsfästs vid felhantering av personuppgifter så länge de rapporterar och samarbetar med relevant instans.

Vidare diskuterade hur användarna kommer att påverkas av den nya förordningen GDPR. Informanten tror att GDPR bara är positivt. Privatpersoner ges en högre benägenhet att faktiskt kunna fråga en verksamhet om informationen som lagras om dem. Det kommer att vara den personuppgiftsansvariges jobb att besvara sådanna frågor. Dessutom kommer i vissa fall "the right to be forgotten" att finnas, där en privatperson kan begära att en verksamhet tar bort all information om privatpersonen i talan.

Intervjun fortsatte med att tala om risk-och sårbarhetsanalyser. Informanten beskrev hur arbetet med risk-och sårbarhetsanalyser bör isolera de system som verkligen måste vara uppe för att ens verksamhet ska fungera. Är det offentlig information kanske det inte ges högst prioritet att isolera jämnfört med ett annat system som behandlar personuppgifter. En fråga verksamheter kan ställa sig är tillexempel: *"Vad händer om denna information läcker ut?"*. Informanten beskrev hur risk-och sårbarhetsanalysen är viktig för att peka på vilken omfattning olika typer av incidenter har på en verksamhet. Det är därefter viktigt att arbeta med att försöka minimera och om möjlig eliminera risken till hanterbara nivåer. Vidare beskrev informanten hur aktiviteter såsom informationsklassning, säkerhetsövervakningstjänster, loggsystem med mera är frågor som dennes företag diskuterar med offentliga verksamheter vid utförande av risk-och sårbarhetsanalys för molntjänster. Informanten nämner Informationsklassning som ett viktigt begrepp *"Vad för information behandlar vi? Vad kan vi lägga upp i molnet? Vad kan vi inte lägga upp i molnet?"*

Avslutningsvis ställdes frågan om vad som händer i dagsläget om en verksamhet inte följer upp sin risk-och sårbarhetsanalys kontinuerligt. Informanten beskrev frågan som extremt bra och förklarade att MSB, Datainspektionen och SKL i dagsläget jobbar väldigt mycket med frågan. Normalt ska en sårbarhetsanalys göras var fjärde år men vissa viktiga verk har ibland som krav på att göra det minst en gång per år. "*I dagsläget kanske Datainspektionen gör ett nedslag vid ett misslyckande, sedan ställas frågor om varför det inte gjorts. Kommer man fram till att organisationen eller företaget grovligen försummat sin datahantering kommer troligvis organisationen att få betala böter, få vitesföreläggande eller annan eftergift".*

4.2 Informant 2 (Expert 2)

Lagar och regler
När vi talade om reglering av information och vilka andra myndigheter de samarbetade med svarade informant 2 att det inte är så mycket av ett samarbete utan att dem är en tillsynsmyndighet enligt personuppgiftslagen. "*Vi granskar andra myndigheter*". Det samarbete som sker är istället i form av att de som myndighet representerar vissa frågor åt andra myndigheter i Bryssel. Däremot arbetar de mycket med förebyggande arbete och tillåter verksamheter att ställa frågor samt begära samråd.
Vidare diskuterades om informanten anser att det råder bristande eller icke tillräcklig reglering i den rådande lagen PuL."*Alltså, det är ju egentligen bristande följdsamhet*. *När någon inte följer reglerna är det främst beroende på bristande kunskap*" beskrev informanten.

Informanten fick även en fråga om hur processen ser ut i dagsläget om en verksamhet som bör uppfylla PuL inte gör detta. "*Ja alltså, om man inte följer regelverket har den personuppgiftsansvarige ett ansvar gentemot den registrerade. Det innebär bland annat ett skadeståndsansvar*".

Informanten svarade även på frågor om GDPR angående hur de förbereder sig inför förändringarna, vad som kommer att skilja sig i deras arbete jämfört med tidigare, samt hur GDPR kan komma att påverka verksamheter i Sverige.
Frågorna genererade följande svar: "*Vi håller just nu på att gå igenom alla delar av förordningen och ställa det gentemot vad som gäller idag, det är ofta mycket gemensamhetsprocesser som ska på plats, vilket vi är ovana vid*". Informanten beskrev att det framförallt handlar om ökade skyldigheter. "*Tidigare skulle man bara följa lagen, nu måste man också på ett mera uttryckligt sätt visa att man faktiskt följer lagen och hur det görs*". Vidare beskrev informanten att ett sett att visa att man faktiskt följer lagen kommer göras genom att verksamheterna kommer vara tvungna att skapa ett register. Registrets syfte är att tydligt förklara hur verksamheten använder personuppgifter. Det finns ingenting idag som talar om att man behöver visa hur lagen följs avslutade informanten med.

Internationellt beskrev informanten att den största förändringen är att förordningen GDPR blir en rättighet i samtliga EU länder. Anledningen till att den nuvarande personuppgiftslagen ersätts av GDPR beskrevs av informanten ur ett rättsligt perspektiv "*PuL är baserat på EU-direktiv från 1995. Dock är det ett direktiv, vilket innebär att det nationella genomförandet ser olika ut. GDPR är en förordning vilket innebär att alla systermyndigheter i Europa måste tillämpa, förstå och tolka förordningen på exakt samma sätt överallt. "Internationellt kommer man framförallt att märka av att informationshantering av personuppgifter underlättas för aktörer som är verksamma i flera olika länder inom EU".* Informanten beskrev även hur detta nationellt kommer innebära att GDPR går före Svensk grundlag.

Vidare fortsatte intervjun med att informanten besvarade en fråga angående hur användarna påverkas av den nya förordningen. Svaret blev att förordningen kommer att underlätta för den registrerade att hävda sina rättigheter. "*Registrerade har större möjlighet i den mån som de känner att det finns oegentligheter hävda sin rätt enligt förordningen*".

Avslutningsvis ställdes en fråga om vad som sker om ett dataintrång inträffar på en offentlig verksamhet som behandlar personuppgifter, med fokus på vem som tar ansvar för

rapporteringen av dataintrånget. Informanten inledde med att nämna att det i dagsläget vanligvis görs en polisanmälan vid dataintrång, men att det inte finns några krav på att det måste göras. Den nya förordningen GDPR kommer främst att reglera så kallade "it incidenter" och inte dataintrång som är ett brott som ska rapporteras till polisen. "*Vid IT incidenter som går till följd av att personuppgifter kan komma på avvägar eller riskerar att komma på avvägar finns det olika krav enligt GDPR att rapportera det till Datainspektionen beroende på allvarlighet*".

4.3 Offentliga verksamheter

Molntjänster

Inledningsvis frågade vi informanterna om hur långt de ansåg att deras offentliga verksamhet hade kommit i sin digitalisering. Alla informanterna konstaterade att det var svårt att jämnföra sig med andra offentliga verksamheter och hade olika åsikter om var de befann sig. Informant 3 uttryckte sig enligt följande:

"Det är svårt att jämföra sig, vi har kommit olika långt inom olika områden, men alla som är anställda har oavsett var de jobbar tillgång till en egen inlogg och epost och ska kunna nås var de än är i världen." **– Informant 3**

Informant 4 ansåg även att de inte riktigt visste var de befann sig och nämnde att en del bolag inom kommunen har kommit långt medan andra ligger och släpar:

"Vi är någonstans i mitten, inte längst fram men inte längst bak." **– Informant 4**

Informant 5 delade samma uppfattning, men nämnde att de var tidiga med att gå ut i molnet:

"Svårt att säga hur långt andra verksamheter har kommit, men vi var tidiga som statlig myndighet att upphandla en molntjänst och mycket tid lades ner på säkerheten." **– Informant 5**

Efter att vi tagit reda på hur långt de offentliga verksamheterna hade kommit i sin digitalisering bad vi informanterna kort berätta om hur arbetet gått tillväga vid införskaffandet av molntjänster. Alla informanter beskrev att de först kontaktade datainspektionen för att se över vilka krav som behövde uppfyllas för att kunna lägga personuppgifter i molnet. Informanterna fick därefter omförhandla molntjänstleverantörernas standardavtal för att uppnå datainspektionens krav. Detta beskrev samtliga informanterna som det jobbigaste arbetsmomentet.

"Det jobbigaste arbetsmomentet var avtalen och att kunna reglera avtalen så att de stämde överens med våra krav. I början var det lite fel på molntjänstleverantörens avtal och vi fick dom att ändra sig, enligt de krav som ställdes." **– Informant 3**

Även informant 4 beskrev att det fanns problem med molntjänstleverantörernas avtal:

"Man måste upp på en rätt hög nivå och det är kämpigt eftersom mycket juridik står ivägen. Det är tufft att hitta rätt nivå på de man pratar med på de större molntjänstleverantörsföretagen." **– Informant 4**

Enligt informant 5 som också anser att det jobbigaste arbetsmomentet är att uppnå datainspektionens krav leder molntjänstleverantörernas färdiga paket till problem, men ansåg att det viktigaste är hur informationen hanteras.

"Förutom avtalsproblematiken gör de färdigpaketerade molntjänsterna att man inte kan skräddarsy det man vill ha. Dessutom gör leverantören uppgraderingar och förändrar tjänsten. Även om avtalen är omfattande är det viktigaste att vi vet vem som äger informationen, hur de hanterar personuppgifter och om de lämnar ut vår information." – **Informant 5**

Vidare ställdes frågor till informanterna angående varför de valde att påbörja användningen av molntjänster. Informanternas generella inställning var att de gjordes på grund av ekonomiska fördelar och för att de själva inte kan uppnå den säkerhet som molntjänstleverantörer erbjuder. Den allmänna inställningen till fortsatt användning av molnet var därför positiv. Informant 5 beskrev arbetet på följande sätt:

"Vi behövde byta ut kontorsstödet i verksamheten och såg ekonomiska fördelar samt säkerhetsfördelar med molntjänster och valde därför att påbörja upphandlingen." **– Informant 5**

Informant 4 tankar om varför de valt att påbörja användningen av molntjänster stämmer överens med resterande förutom att de även beskrev att kapaciteten har varit en viktig påverkande faktor.

"Det kan kostnadsmässigt samt säkerhetsmässigt bli en vinst, den främsta anledningen är däremot att vi själva inte har kapaciteten att upprätta samma säkerhet som stora företag. Att få ihop säkerheten på deras nivå kostar mängder för oss, men är enkelt för dom. Därför finns det en anledning att överväga molntjänster i varje nytt område vi tittar på". – **Informant 4**

Lagar och regler

Vi frågade även om informanternas inställning till den nuvarande personuppgiftslagen (PuL) för att ta reda på om de anser att de råder en bristande reglering i lagen. Alla informanterna ansåg att det inte är några brister i lagen, men att det precis som vid upphandlandet av molntjänster gäller att hamna på rätt nivå.

"För att nå upp på nivån tog verksamheten hjälp av juridisk expertis som var med hela tiden och svarade på de svåra frågorna angående personuppgiftshantering" **- Informant 4**

Därefter frågade vi de offentliga verksamheterna om hur arbetsprocessen går till om personinformation läcker ut från verksamheten eller felbehandlas. Alla informanter anser att det är säkert att lägga informationen i IT-lösningar då de har en bra uppsyn över hur information rör sig i dessa lösningars loggar. Informanternas beskrivning av hur de arbetar om data förlorats stämmer till en viss del överens, men de beskrev ändå olika tillvägagångssätt.

Informant 3 nämnde att det första steget handlar om att stoppa det som har hänt och därefter kolla igenom loggarna. Hur händelsen åtgärdas skiljer sig senare efter att det klartgjorts vad för typ av missbruk det rör sig om.

"*Oftast är det en medveten handling och då har man inte följt reglerna, om någonting olagligt sker så görs en polisanmälan.****"*** **– Informant 3**

Att anmäla ett brott till polisen ansåg även informant 4 vara ett vanligt sätt att hantera dessa typer av händelser på. De har dessutom incidentprocesser som fångar in störningarna.

"*Vi har alltid egna utredningar, om det inte är ett brott så utreder vi själva. Till exempel kan det handla om att informationen inte läggs undan på rätt sätt.****"*** **– Informant 4**

Informant 5 sa till skillnad från tidigare informanter ingenting om en polisanmälan. Istället beskrev informanten att de har filter och brandväggar som kontrollerar all trafik och att molntjänstleverantören har en skyldighet att rapportera in incidenter till dom.

"*Vi har väldigt bra kontroll och molntjänstleverantören får självklart rapportera in incidenter till oss så utreder vi det sedan"* **- Informant 5**

Den nya förordningen GDPR var i fokus i nästkommande frågor. Vi inledde med att fråga hur informanterna förbereder sig inför de nya bestämmelserna. Detta för att se vilka förändringar de offentliga verksamheterna förväntas behöva genomföra i deras arbetssätt.
Flera av informanterna beskrev att de inte är familjära med lagen och menade att den främst kommer att påverka den juridiska avdelningen. Det här skiljer sig från Informant 3 uppfattning som beskrev att den största skillnaden kommer handla om att det blir ett högre krav för deras verksamhet att kunna bevisa vad syftet är med att använda sig den data som deras verksamhet behandlar. Informanten menar att detta behöver göras för att förbättra förstörandet av data snarare än lagringen av det.

"*Det ska finnas en rätt att bli glömd eller right to be forgotten. Just nu handlar det för mycket om säkerhetsrisker med molntjänster, det ska snarare handla om hur gammal information ska gallras.****"*** **– Informant 3**

Förutom att den juridiska avdelningen kommer påverkas påpekar informant 4 även att förordningen kommer att ställa krav på leverantören.

"*Just nu är vi ansvariga för att se till att hanteringen av de personuppgifter som ligger i molnet hanteras korrekt, men det kommer att vara molntjänstleverantören uppgift också. Alla ska vara med och stå på tå, just nu är det vi som får se till att leverantören står på tå."*
– Informant 4

Tidigare har det inte funnits någon skyldighet att rapportera in felhanteringen av personuppgifter. När förordningen införs kommer det däremot att bli ett nytt krav. Vi frågade därför informanterna om de idag faktiskt kan se om någon har kommit åt eller missbrukat personuppgifter i verksamheten. Alla informanter sa att de redan idag har incidentprocesser på plats och att de kan rapportera in informationen om det behövs.

"*Jag tror inte att en rapportering inom en viss tid eller att ha en skyldighet att rapportera in incidenter kommer att bli ett problem för oss"* **- Informant 4**

GDPR kommer även att införa en straffavgift som kan tillämpas om verksamheter inte följer den nya förordningen. Vi frågade därför informanterna om de anser att straffavgiftens storlek

på 2-4% av en koncerns globala omsättning är rimlig. Alla informanter hoppades att lagen främst kommer att användas för att avskräcka verksamheter från att inte följa förordningens krav på hanteringen av personuppgifter. Detta då storleken på straffavgiften uppfattades som väldigt hög.

"*Straffavgifter bör sättas i relation till den skada som uppstått i förhållande till den drabbade och utifrån detta sättas med en rimlig nivå. Om lagen används i avskräckande syfte, eller främst för att se till att verksamheter följer förordningen kan man förstå det, men de bör även ha i åtanke vilka säkerhetsåtgärder som har vidtagits och om man försökt att förhindra händelsen."* **– Informant 5**

Offentliga verksamheter kommer även i och med införandet av GDPR vara tvungna att anställa ett dataskyddsombud som enbart arbetar med personuppgiftshantering. Därför undrade vi om informanterna har någon sådan person idag. Informanternas tolkning var att de inte handlar om att anställa en ny person utan att den som i dagsläget är personuppgiftsansvarig kommer att få högre krav. Hur de svarade på frågan skiljer sig dock till en viss del. Informant 3 verkade mer oroad inför förändringen och svarade:

"*Vi måste se över detta och anpassa verksamheten till den nya förändringen."* **– Informant 3**

Informant 4 och 5 uppfattades däremot som mindre oroliga.

"*Det hela är nog försumbart när vi pratar om en enda tjänst.****"*** **– Informant 4**

"*Jag tror inte att det blir en extra uppgift, vi har redan idag en personuppgiftsansvarig som ansvarar för liknande frågor."* **– Informant 5**

Vidare frågade vi vad informanterna tycker om det potentiella extra arbetet som GDPR för med sig jämfört med PuL och ifall förordningen kommer att innebära några fördelar. Överlag anser samtliga informanter att förändringen är positiv, men har olika tankar om hur de kommer att dra nytta av förändringen.

Informant 3 tycker att förändringen stärker motiven för att på ett korrekt sätt arbeta med hanteringen, bevaringen och gallringen av personuppgifter. Detta då förordningen ställer krav på verksamheter att kunna redovisa hur personuppgifter hanteras.

"*Ordning och reda är ett krav som funnits tidigare, detta ger dock den enskilde möjligheten att se till att detta sker.* **– Informant 3**

Till skillnad från informant 3 var informant 4 tveksam över hur många extramoment förordningen kommer att innebära, men tyckte att förändringen är positiv för att EU ställer högre krav på leverantörerna av molntjänster.

"*Det finns ingen som kan ducka, jag ser bara positivt på det, utifrån vad jag vet."*
– Informant 4

Informant 5 svarade att det är bra att ha ordning och reda samt brukar tänka att om någon annan har tänkt till så borde lösningen gagna alla.

"På något sätt kommer vi att dra nytta av att vi har gemensamma regler, allt med säkerhetsarbete är ju medarbete men de måste ju motivera det med någon form av enhetlighet. Vi kan också känna oss trygga när vi vet att andra verksamheter behandlar personuppgifter på rätt sätt." **– Informant 5**

Efter att vi frågat informanterna om GDPR talade vi med informanterna om deras arbete med sårbarhetsanalyser. Detta för att få en förståelse för hur verksamheterna arbetat med sådana vid införandet av molntjänster.
Informanterna berättade om arbetsprocesserna olika, men alla informanter ansåg att det viktigaste arbetet med risk och sårbarhetsanalysen handlade om kartläggningen av risker. Det som skiljer sig åt är istället hur leverantören var involverad i arbetet.

Informant 3 nämnde att deras molntjänstleverantör endast ansvarade för en liten del i arbetet och att verksamheten var ansvarig för att göra arbetet rätt:

"Det viktigaste med analysen är att veta vilka risker man är medveten om. Vi genomförde arbetet med olika personer inom olika delar av verksamheter för att säkerställa detta."
– Informant 3

På frågan om hur de arbetar med sårbarhetsanalyser svarade informant 4 att de främst arbetade med en riskanalys för att i ett senare skede göra en sårbarhetsanalys för relevanta risker. Till skillnad från informant 3 så kompletterades arbetet med riskerna av molntjänstleverantören innan de genomförde analysen:

"*Informationskartläggningen gjordes först. Sen gjorde vi en kravbildsanalys där vi tog med interna och externa krav. Efter processerna kompletterats med informationen från leverantören genomförde vi sårbarhetsanalysen."* **– Informant 4**

Informant 5 sa att de satte upp en workshop med säkerhetschefen, huvudjuristen och två duktiga tekniker. Därefter brainstormade man fram risker och gjorde en analys på hur troligt de är att de skulle inträffa samt vilken skada risken skulle ge:

"*Frågorna vi ställde oss var: Vilka krav behöver ställas? Går detta att lösa tekniskt? Administrativt? Utifrån detta togs sedan en rapport fram där vi förklara hur vi arbetat."*
– Informant 5

Samtidigt ville vi ta reda på om sårbarhetsanalyserna öppnade upp informanternas ögon för problem som de tidigare inte tänkt på. Informanterna beskrev generellt att man redan kände till resultatet man fick fram, men att det fanns en del intressanta aspekter i arbetet. Detta då arbetssättet ledde till en diskussion mellan individer som besatt olika kompetenser om hur stor sannolikheten är att någonting inträffar.

Informant 4 beskrev användarna som den helt klart största risken:

"Vi kan sätta på hur mycket säkerhet som helst, det hindrar inte användarna från att kunna göra tokiga saker. Tänk om en användare skickar mail med något hemligt i, det kan man ändå inte skydda, vare sig det är en molntjänst eller inte." **– Informant 4**

Avslutningsvis frågade vi om det är någonting i arbetet med risk- och sårbarhetsanalysen som skiljer sig vid införskaffningen av en molntjänst jämfört med vanliga risk- och

sårbarhetsanalyser. Förutom att informanterna behövde förhålla sig till PuL så beskrevs det inte vara några större skillnader.

> *"Vi behövde göra allting 100 % rätt i förhållande till PuL, men skillnaden i arbetet med riskanalysen var inte nämnvärt stor. Vi följde även en annan verksamhets risk- och sårbarhetsanalys vid upprättningen av vår egna då vi visste att de fått arbetet godkänt av datainspektionen. Analysen fick dock modifieras på så sätt att vi lade till egna frågor om säkerhetsarbetet."*– **Informant 4**

5. Resultatanalys och diskussion

Uppsatsens syfte var att besvara frågeställningen "*Vilka faktorer är viktiga för offentliga verksamheter att beakta i och med övergången till den nya förordningen GDPR?"*
För att besvara frågan har de två experternas utlåtanden samt de tre offentliga verksamheternas svar på de frågor som ställdes under intervjuerna analyserats. Resultatet kopplas även till studiens tidigare framställda bakgrund och teori.

IFI (2010) beskriver att allt fler offentliga verksamheter väljer att använda sig av IT. Detta återfinns även i vårt empiriska resultat där det framkommer att de tre offentliga verksamheterna vi talade med till en viss del använder sig av IT-lösningar. En av de IT-lösningar som de offentliga verksamheterna använder sig av är molntjänster.

I vår teori framställs många olika fördelar med att gå ut i molnet. Några av dessa fördelar är att kunna ta del av en tjänst eller produkt via Internet istället för att verksamheten själv äger den. En annan anledning till att gå ut i molnet är att verksamheten oftast sparar pengar och minskar sitt administrativa arbete (Greenwood et al. 2011; Corbett 2004; Subhankar 2012).
Det framkom av informanterna från de offentliga verksamheterna att de främst valt att använda sig av molntjänster på grund av de ekonomiska fördelarna. Samtidigt nämnde alla informanter att säkerhetsaspekten varit en viktig del i valet av att använda molntjänster. De beskrev att de själva inte hade kapacitet nog för att uppnå den säkerhet som molntjänstleverantörerna kan erbjuda. Detta går även att återfinna i vår teori där det beskrivs hur verksamheter i vissa fall kan uppnå en större säkerhet genom att gå ut i molnet (Naser 2015). Det beskrivs dock även hur man borde finna en balans mellan den ekonomiska nyttan med att gå ut i molnet utan att äventyra säkerheten då det även finns säkerhetsrisker i molnet (NIST 2011).

Det är alltid viktigt att följa lagar och regler, inte minst för offentliga verksamheter. Avseende reglering av personuppgifter måste i dagsläget offentliga verksamheter därför följa personuppgiftslagen vid införskaffande av molntjänster (Datainspektionen u.å.d). I vår teori beskrivs även att det uppstår legala problem för offentliga verksamheter vid införskaffande av molntjänster då de inte längre har full kontroll över sin information (Karlsson 2014; Datainspektionen u.å.c). Detta beskrivs även i det empiriska resultatet där expert 1 nämner att det som stoppar eller fördröjer processen för offentliga verksamheter från att gå ut i molnet är de legala frågorna. Det framkom även i empirin att de offentliga verksamheterna upplevde de legala aspekterna som de jobbigaste arbetsmomenten. Till exempel ansåg informanterna att molntjänstleverantörernas standardavtal var problematiska då de inte uppfyllde PuL. Samma problem går att återfinna i vår teori som beskriver att verksamheter behöver omförhandla standardavtalen för att uppfylla de lagkrav som ställs (NIST 2011; Brodkin 2008; Datainspektionen u.å.c; Karlsson 2014).

När vi talade om hur processen i dagsläget ser ut vid rapportering av felhanterad eller försvunna personuppgifter i offentliga verksamheter nämnde experterna att det idag inte finns något krav på hur rapporteringen ska gå till. Experterna beskrev att det i dagsläget vanligaste sättet att rapportera dataintrång är att göra en polisanmälan och att det inte finns några bestämmelser för exakt hur förlust eller felhantering av personuppgifter ska rapporteras. Detta går även att urskilja i de offentliga verksamheternas uttalanden.
En av informanterna nämnde att de vanligtvis gör en polisanmälan om de misstänker ett brott. En annan informant beskrev också att de gör en polisanmälan, men att de även tillsätter en egen utredning av incidenten. Ytterligare ett sätt rapporteringen beskrevs på var att den offentliga verksamhetens molntjänstleverantör rapporterar incidenten till verksamheten. Sedan görs en intern utredning inom den offentliga verksamheten. Vår empiri belyser alltså en brist i enhetliga riktlinjer för hur incidentrapportering ska gå till. Detta då informanterna beskriver ganska olika tillvägagångssätt.

I vårt bakgrundsavsnitt beskriver vi att man som verksamhet i och med införandet av GDPR kommer ha skyldighet att rapportera in förlust av personuppgifter till en tillsynsmyndighet (Delphi 2016; Datainspektionen 2016a). Detta beskrevs även av experterna vara en av de största förändringarna för offentliga verksamheter som hanterar personuppgifter. Informanterna från de offentliga verksamheterna upplevde däremot att de redan i dagsläget har avancerade loggsystem som kan rapportera in felhantering av personuppgifter om det behövs. Informanterna ansåg därför att incidentrapportering inte kommer vara ett problem i och med införandet av GDPR. Detta stämmer inte överens med hur expert 1 uppfattade problemet. Enligt experten var en av de största utmaningarna för verksamheter att kunna skapa loggar och arbetsrutiner för att kunna upptäcka att de blivit av med personuppgifter. I empirin framkom även av expert 2 att det i GDPR finns krav på att kunna rapportera in förluster av personuppgifter till skillnad från tidigare. Bara för att informanterna från de offentliga verksamheterna har loggsystem som beskrivs kunna fungera för rapportering idag, behöver det inte betyda att de är tillräckliga när GDPR genomförts. Baserat på expertutlåternas svar samt informanternas tidigare beskrivning av att de endast gör en polisanmälan eller tillsätter en intern utredning, rekommenderar vi därför offentliga verksamheter att se över sitt sätt att rapportera in incidenter. Detta skulle kunna göras genom att de offentliga verksamheterna redan idag tar fram riktlinjer för hur incidenterna ska rapporteras in i framtiden. De kan även redan nu börja testa att rapportera in incidenter i en mindre skala för att se hur systemen fungerar.

Som vi tagit upp i bakgrundsavsnittet kan individer i dagsläget begära skadestånd enligt PuL om denne kan bevisa att verksamheten misskött hanteringen av hans eller hennes personuppgifter. I och med GDPR kommer även en administrativ avgift för verksamheter som missbrukar hantering av personuppgifter att införas. Den administrativa avgiften kommer uppgå till 2-4 % av en koncerns globala omsättning, vilket framgår i vårt bakgrundsavsnitt (Delphi 2016; Datainspektionen u.å.d). I empirin framkom att informanterna från de offentliga verksamheterna hoppas att boten främst kommer användas i ett avskräckande syfte för att se till att regleringen följs. Detta då botens storlek uppfattas som väldigt hög. Expert 1 beskrev att boten kommer vara viktig för offentliga verksamheter att tänka på i och med införandet av GDPR. Baserat på expert 1 svar och informanterna från de offentliga verksamheternas inställning till botens storlek anser vi att det är en viktig faktor att beakta. Detta då boten kan påverka de offentliga verksamheterna negativt eftersom det handlar om stora belopp. För att undvika boten skulle offentliga verksamheter kunna skapa arbetsrutiner som gör att det blir svårt att felbehandla personuppgifter. Till exempel skulle de kunna använda sig av ett loggsystem för att se till att ingen i verksamheten gör något som inte är

tillåtet med personuppgifterna. De skulle även kunna skapa en miljö i systemet som inte tillåter att personuppgifter förflyttas eller kopieras utan tillåtelse.

Vi beskriver i bakgrundsstycket att verksamheter kommer behöva tillsätta en ny roll, vilket är ett dataskyddsombud. Dataskyddsombudet kommer vara en speciellt anställd med ansvar för personuppgiftshantering och praxis (Delphi 2016; Datainspektionen 2016a). Förutom att ta hand om personuppgifter framgår även i vår bakgrund att dataskyddsombudet kommer ansvara för ett nytt register. Registret ska innehålla tydlig information om hur verksamheten behandlar personuppgifter. Expert 2 beskriver även likt vår bakgrund till studien att registret kommer upprättas för att verksamheter tydligare ska visa att de följer lagen jämfört med tidigare. När informanterna från de offentliga verksamheterna uttalade sig om det nya dataskyddsombudet framgick att de inte kände till förändringen. Informanterna antog därför att personuppgiftsombudet kommer att anta den nya rollen, vilket inte stämmer överens med Delphi (2016) och Datainspektionen (2016a) beskrivning i vår bakgrund. Vårt empiriska resultat pekar alltså på att en kompetensutvärdering bör göras. Exempelvis kan den som idag är personuppgiftsombud kanske vidareutbildas för att kunna anta den nya rollen. Ett annat alternativ är att anlita en extern person som tar på sig rollen som dataskyddsombud.
Offentliga verksamheter skulle även redan idag kunna försöka upprätta ett register där det de beskriver hur personuppgifter hanteras inom verksamheten för att vara redo för den kommande förändringen.

6. Slutsats

I vår studie har vi sökt svaret på följande frågeställning "*Vilka faktorer är viktiga för offentliga verksamheter att beakta i och med övergången till den nya förordningen GDPR?"* Genom samtal med olika intressenter har vi i studien identifierat viktiga faktorer som offentliga verksamheter bör beakta i och med den nya förordningen. De faktorer som framkom är framtagna från skiljaktigheter i hur vissa processer ser ut idag och hur de kommer att se ut i framtiden.

Den första faktorn som är viktig för offentliga verksamheter att beakta i och med övergången till den nya förordningen GDPR är den administrativa avgiften vilket ställer krav på verksamheter att följa de nya bestämmelserna kring personuppgiftshantering.
Framtagande av arbetsrutiner och väl fungerande system som underlättar personuppgiftshantering är viktiga aspekter att se över för att undvika boten.

Den andra viktiga faktorn handlar om att offentliga verksamheter kommer ha ett krav på sig att kunna incidentrapportera förluster eller felhantering av personuppgifter till landets tillsynsmyndighet. Att redan idag skapa klara riktlinjer för hur incidenter ska rapporteras in samt testa att rapporteringen faktiskt fungerar anses viktigt för framtiden.

Den tredje faktorn är uppdelad i två delar. Första delen handlar om att offentliga verksamheter kommer vara tvungna att tillsätta en ny roll i form av ett dataskyddsombud som ansvarar för personuppgiftshanteringen i verksamheten. Kompetensutvärdering och vidareutbildning av befintlig personal, alternativt att köpa tjänsten av utomstående är två alternativ som kan ses över. Den andra delen handlar om att verksamheter kommer behöva upprätta ett register. Detta register ska beskriva hur personuppgifter används i verksamheten och kommer vara dataskyddsombudets ansvar. Registret kan redan idag upprättas av de offentliga verksamheterna för att de ska vara väl förberedda inför förändringen.

Det kommer vara intressant att följa offentliga verksamheters arbete med övergången till GDPR de kommande två åren. Detta då de ovanstående faktorerna kommer ha en stor inverkan på offentliga verksamheters personuppgiftshantering i molnet.

Referenslista

Armbrust, M., Fox, A., Griffith, R., Joeph, A., Kantz, R., Kowinski, A., Lee, G., Patterson, G., Rabkin, A., Stocia, I., Zaharia, M. (2010). A View of Cloud Computig - Clearing the clouds away from the true potential and obstacles posed by this computing capability. 53(4) ss. 50.

Braun, V. & Clarke, C. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2) ss. 77-101. DOI: 101.1191//1478088706qp063oa

Brodkin, J. (2008). Gartner: Seven cloud-computing security risks - Data integrity, recovery, privacy and regulatory compliance are key issues to consider. http://www.networkworld.com/article/2281535/data-center/gartner--seven-cloud-computing-security-risks.html [2016-04-15]

Columbus, L. (2014). Roundup Of Cloud Computing Forecasts And Market Estimates Q3 Update. Forbs Magazine. http://www.forbes.com/sites/louiscolumbus/2015/09/27/roundup-of-cloud-computing-forecasts-and-market-estimates-q3-update-2015/#3cc05eaf6c7a [2016-03-08]

Computer Sweden (2013). Kommunal IT svämmar över. http://computersweden.idg.se/2.2683/1.496030/kommunal-it-svammar-over [2016-04-19]

Corbett. M (2004). The Outsourcing Revolution. Economist. https://www.economist.com/media/globalexecutive/outsourcing_revolution_e_02.pdf [2016-05-11]

Datainspektionen. (2016a). EU:s dataskyddsreform. http://www.datainspektionen.se/lagar-och-regler/eus-dataskyddsreform/#1 [2016-06-05]

Datainspektionen. (2016b). Integritet i fokus. Stockholm: Datainspektionen. http://www.datainspektionen.se/Documents/integritetifokus/integritet-i-fokus-16-01.pdf

Datainspektionen. (u.å.c) Molntjänster och personuppgiftslagen. http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/molntjanster/ [2016-04-22]

Datainspektionen (u.å.c) Personuppgiftslagen. http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/ [2016-04-22]

Datainspektionen. (u.å.e). Om Datainspektionen. http://www.datainspektionen.se/om-oss/ [2016-05-22]

Delphi. (2016). Ny Personuppgiftslag, snart verklighet. [PPT] Föreläsning advokatfirman Delphi. [Internt material]

Dubey, A., Wagle, D. (2007). Delivering software as a service - The Mckinsey Quarterly: The Online Journal of McKinsey & Co. http://www.executivesondemand.net/managementsourcing/images/stories/artigos_pdf/sistemas_informativos/Delivering_software_as_a_service.pdf

European Commission. (2012). Commission staff working paper - executive summary of the impact assessment. Bryssel: European Commission. http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf

Europeiska Unionen. (u.å.). Förordningar, direktiv och andra rättsaker. http://europa.eu/eu-law/decision-making/legal-acts/index_sv.htm [2016-04-22]

Europeiska Kommissionen. (2012). Rapport från kommissionen till europaparlamentet, rådet, europeiska, ekonomiska och sociala kommittén samt regionkommittén. Bryssel: Europeiska Unionen. http://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:52012DC0012&from=SV

Europeiska Kommissionen. (2015). Överenskommelse om kommissionens reform av EU:s uppgiftsskydd stärker den digitala inre marknaden (Pressmeddelande från EU IP/12/46 http://europa.eu/rapid/press-release_IP-15-6321_sv.htm

Fernandes, D., Soares, L., Games, J., Freire, M., Inácio, P. (2013). Security issues in cloud environments: a survey. International Journal of Information Security, 13 ss. 113-170. DOI: 10.1007/s10207-013-0208-7

Holmström, M. (2013). Instimt samarbete mellan FRA och NSA. Svenska Dagbladet. http://www.svd.se/intimt-samarbete-mellan-fra-och-nsa/om/sverige [2016-03-08]

IFI. (2010). IT-sourcing i offentlig sektor - omfattning, inriktning och trender. http://www.ifi.se/rapport-unik-kartlaggning-av-it-i-offentlig-sektor [2016-04-20]

International Business Times. (2015). Top European Court Kills “Safe Harbor”. A Major Blow To Us Tech Companies Like Google, Microsoft and Facebook. http://www.ibtimes.com/top-european-court-kills-safe-harbor-major-blow-us-tech-companies-google-microsoft-2128640 [2016-04-21]

Kazim, M., Zhu, S.Y. (2015). A survey on top security threaths in cloud computing. International Journal of Advanced Computer Science and Applications, 6(3) ss. 109-113

Karlsson, N. (2014). Risker vid personuppgiftsbehandling i digitala molntjänster. Masteruppsats, Juridiska institutionen. Stockholm: Stockholms Universitet.

Khajeh-Hosseini, A., Greenwood, D., Smith, J., Sommerville, I. (2011). The Cloud Adoption Toolkit: Supporting cloud adoption decisions in the enterprise. School of Computer Science,University of St Andrews, 42 ss. 447-465 DOI: 10.1002/spe.1072

Leduc. (2007a). Metodhandbok som tankekarta http://www.leduc.se/metod/Induktion,deduktionochabduktion.html [2016-05-03]

Leduc. (2007b). Metodhandbok som tankekarta. http://www.leduc.se/metod/Validitetochreliabilitet.html [2016-05-03]

Lee, K. (2012). Security Threats in Cloud Computing Environments. International Journal of Security and Its Applications, 6(4) ss. 25-32.

Libell, H. (2013). Prognos för offentlig sektor: Molnigt med en chans för IT som en tjänst. Masteruppsats, Institutionen för tillämpad informationsteknologi. Göteborg: Göteborgs Universitet.**http://hdl.handle.net/2077/33895**

Long, J,W., Quek, P, M. (2002). Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise. Journal of European Public Policy, 9(4) ss. 325-344. DOI: 10.1080/13501760210138778

Marston, S., Li, Z., Bandypadhyay, S., Ghalsasi, A. (2011). Cloud Computing - The Business Perspective: 44th Hawaii International Conference on System Sciences, 51(1) ss. 176-189. DOI: 10.1016/j.dss.2010.12.006

Myndigheten för samhällsskydd och beredskap. (2015a). Risk- och sårbarhetsanalyser. Karlstad: Myndigheten för samhällsskydd och beredskap. https://www.msb.se/RibData/Filer/pdf/27577.pdf

Myndigheten för samhällsskydd och beredskap. (2011).Vägledning för risk- och sårbarhetsanalyser. Karlstad: Myndigheten för samhällsskydd och beredskap. https://www.msb.se/RibData/Filer/pdf/25893.pdf

Naser, S., Kamil, S., & Thomas N. (2015). A Case Study in Inspecting the Cost of Security in Cloud Computering. School of Computing Science, Newcastle University, 138, ss. 179-196. DOI: 10.1016/j.entc.2015.10.026

Nationalencyklopedin (2016). IT. http://www.ne.se/uppslagsverk/encyklopedi/lång/it [2016-04-21]

National Institute of Standards and Technology. (2011). Guidelines on Security and Privacy in Public Cloud Computing. Gaithersburg: NIST. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

National Institute of Standards and Technology. (2011). The NIST Definition of Cloud Computing. Gaithersburg: NIST. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Patel, R. & Davidson, B. (2011). Forskningsmetodikens grunder: Att planera, genomföra och rapportera en undersökning. Lund: Studentlitteratur

Post och Telestyrelsen. (2015). Svenskarnas användning av telefoni och internet, individundersökning. (Rapport PTS-ER-2015:29). Stockholm: Post och Telestyrelsen. https://www.pts.se/upload/Rapporter/Tele/2015/individundersokning-2015-pts-er-2015_29.pdf

Rensfeldt, G. (2013). FRA hackar datorer - Topphemligt projekt med NSA. SVT, Uppdrag granskning. http://www.svt.se/ug/fra-hackar-datorer [2016-03-08]

Riley, P & Tamkin, P. (1996). Outsouring: A Flexible Option for the Future?

Brighton: The Institute for Employment Studies.

Shields, P & Rangarajan, N. (2013). A Playbook for Research Methods:. Integrating Conceptual Frameworks and Project Management. Stillwater: New Forums Press

SKL. (2014). E-tjänster och appar - hur är läget i kommunerna? E-förvaltning och E-tjänster i Kommunerna. Stockholm: Sveriges Kommuner och Landsting.

http://www.internetstatistik.se/wordpress/wp-content/uploads/2014/09/skl-undersokning-2014-etjanstappar.pdf

Stenvall, H. (2014). Företagens förtroende för säkerheten i molnet rekordlågt. Skydd & säkerhet. http://skyddosakerhet.se/nyheter/foretagens-fortroende-sakerheten-molnet-rekordlagt/ [2016-03-09]

Subhankar, D. (2012). From outsourcing to Cloud computing - evolution of IT services. Management Information Systems, 35(8), ss. 664-675. DOI: http://dx.doi.org/10.1108/01409171211247677

Tieto (2016). Molnet vinner mark i kommunerna. https://www.tieto.se/trender-och-insikter/molnet-vinner-i-kommun-it [2016-04-20]

Winston & Strawn. (2015). EU Court of Justice Kills Safe Harbor. Privacy and Data Security Practice. Winston & Strawn. http://interact.winston.com/reaction/IntellectualProperty/ClientBriefingNewsletter/2015/EUCrtJusticeKillsSafeHarbor_OCT2015/EUCrtJusticeKillsSafeHarbor_OCT2015.pdf

Åsberg, R. (2001). Det finns inga kvalitativa metoder och inga kvantitativa heller för den delen - det kvalitativa-kvantitativa argumentets missvisande retorik: Institutionen för pedagogik och didaktik, Göteborgs Universitet 6(4) ss. 270-292.

Bilaga 1 – Intervjumall säkerhet och försäljningschef

Öppningsfråga
– Hej! Tack för att du tagit dig tiden att prata med oss. Vilken roll har du på företaget och hur länge har du arbetat inom det här området ? Erfarenheter?

1 Molntjänster.
– Vilka är de vanligaste molntjänsterna ni erbjuder ?

– Förändrar era kunder sin inställning till molntjänster efter implementationen till skillnad från pre-implementation ?

– Vilka utmaningar anser ni att det idag finns med molnstjänster ?

Följdfråga: Hur ser ni på det här med risker och minskad tillit till molnet? Enligt media har tilliten till molnet minskat på senare år pga av olika omständigheter.

– Måste man rapportera in händelser såsom dataintrång enligt den nya lagen för att undvika böter?

– Kommer GDPR att förändra hur arbetet fungerar med outsourcing gentemot hur det fungerar idag ? Hur kommer ni att förändra ert arbete ?

– Kommer GDPR att öka tilliten till molntjänster igen ?

2 Lagar och Regler,
– Anser ni att det idag råder bristande eller icke tillräcklig reglering i lagen "PuL" angående informationshantering? Isåfall vad?

– Vilka lagar och regler är det som gäller för er verksamhet idag när det kommer till molntjänster ? Finns det någonting som är likt GDPR ?

– Vem har ansvaret för datat som lagras? Är det ni eller företaget som hyr er tjänst? Vad händer i dagsläget ifall känslig information läcker ut? Hur ser då arbetsprocessen ut?

– Vilka av de tjänster som ni arbetar med kommer att påverkas mest av GDPR ?

– Hur tror du att förändringen med hur personinformation ska hanteras i.om införandet av GDPR kommer att påverka Sverige nationellt ?

– Hur påverkas användarna av GDPR, kommer de att uppleva att deras data hanteras bättre ?

– Vilka aktörer anser du har en central roll i arbetet med GDPR nationellt ?
Följdfråga: Kommer GDPR att försvåra det för NSA "USA" att samla information om vad och vem dom vill ?

Följdfråga: GDPR kommer att tillföra en böter som kan utfärdas för verksamheter som inte följer lagen, hur mycket kommer böten att ligga på ?

3. Sårbarhetsanalys
– Vad är en risk och sårbarhetsanalys och vad används den till ?

Följdfråga: Om en kommun anställer er som molntjänstleverantör och behöver upprätta en risk & sårbarhetsanalys. Behöver de även se över hur ni hanterar informationen eftersom att ni är leverantörer av tjänsten ?

– Är det något specifikt som tas upp när en risk och sårbarhetsanalys diskuteras med en kund i samband med molntjänster ?

Följdfråga: Finns det en standard för hur information klassificeras eller skiljer det sig för varje företag ?

– Kommer GDPR påverka hur man arbetar med risk och sårbarhetsanalysen på något sätt?

– MSB beskriver att en sårbarhetsanalys ska tas fram var fjärde år och att den ska följas upp regelbundet. Vad händer om en offentlig verksamhet inte följer upp sin sårbarhetsanalys ?

– Vilken metod använder ni er av när ni upprättar en risk och sårbarhetsanalys för offentliga verksamheter ?
Följdfråga: Är det just personuppgiftshanteringen som kommer att vara bötbar?

Bilaga 2 – Intervjumall säkerhetsspecialist, Datainspektionen

Öppningsfråga

– Hej! Tack för att du tagit dig tiden att prata med oss. Vilken roll har du på datainspektionen och hur länge har du arbetat inom det området ? Erfarenheter?

– Vad är datainspektionens huvuduppgift och vilken auktoritet har ni?

– Hur många instanser ansvarar ni för i Sverige? Vilka ?

– Vilka andra myndigheter samarbetar ni med? På vilket sätt? T.ex Myndigheten för samhällsskydd och beredskap?

1. Lagar och regler

– Vilka övergripande lagar och regler för informationshantering ser ni över idag?

– Anser du att det idag råder bristande eller icke tillräcklig reglering i lagen angående informationshantering av personuppgifter? Isåfall vad?

– Vad skiljer sig mellan en privat och offentlig verksamhet gällande informationshantering av personuppgifter och dess säkerhet?

– Hur ser processen ut i dagsläget för om en verksamhet inte uppfyller eller följer någon av de lagar eller regler som är uppsatta?

– GDPR är på väg att börja gälla i Sverige, kan du berätta lite om hur datainspektionen arbetar med att förbereda sig inför dom förändringarna som den nya förordningen innebär?

– När vi talar om hur ni har arbetat tidigare, vad kommer GDPR att förändra? Vad behöver man veta som offentlig verksamhet?

– Om ett dataintrång på en offentlig verksamhet sker, vem ska det rapporteras till? Vem tar ansvar för rapporteringen av dataintrång?

– Studien har utformats utifrån GDPR och två perspektiv: Internationellt och Nationellt. Hur skulle du kort sammanfatta GDPRs inverkan på dessa perspektiv?

Bilaga 3 – Intervjumall offentliga verksamheter

Den här intervjumallen har använts för alla offentliga verksamheter som deltagit i studien med en viss variation på hur frågorna ställdes. Värt att notera är även att vissa av frågorna inte har ställts under vissa intervjuer då vi uppfattade att intervjupersonen redan svarat på frågan.

Öppningsfråga

– Hej! Tack för att ni har tagit er tiden att prata med oss. Vilken roll har ni på X verksamhet och hur länge har ni arbetat inom det området? Vad har ni för erfarenheter?

1. Molntjänster

– Hur långt skulle ni säga att ni har kommit i er digitalisering?

– Har ni påbörjat arbetet med att gå över till molntjänster? Kan ni isåfall kort berätta om hur arbetet har gått tillväga för att komma dit ni är idag?

Följfråga: Vad är planen för framtiden med molntjänster? Har ni någon plan på att expandera användingen av molnet inom andra områden? Isåfall vad?

– Vad var er inställning till molntjänster innan ni införskaffade tekniken?

– Vilka var de största problemen ni stötte på vid införskaffandet av molntjänster?

2. Lagar och regler

– För att kunna införskaffa molntjänster behöver man arbeta med att få användningen av tekniken godkänd enligt PuL, kan ni beskriva hur det arbetet har gått till?

– Anser ni att det idag råder bristande eller icke tillräcklig reglering i lagen "PuL" angående personuppgiftshantering? Isåfall vad?

– Vem har ansvaret för datan? Vad händer i dagsläget ifall personinformation läcker ut? Hur ser då arbetsprocessen ut?

– EU har klubbat igenom den nya lagen GDPR som kommer börja gälla tidigast 2018 i Sverige. Vi antar att ni är familjära med lagen och vad den innebär. Hur ser ert arbete ut med att förbereda er för de nya direktiven? Är det stora förändringar som behöver göras?

– Tidigare har ingen skyldighet för rapportering av felhantering av persondata funnits, i och med GDPR kommer detta bli en skyldighet. Hur ser ni på detta? Har ni idag kapaciteten att faktiskt se om någon kommit åt personinformation?

– Anser ni att straffavgiften är rimlig? Hur kommer ni att arbeta för att undvika avgiften? (Staffavgiften är på 2-4% av en koncerns globala omsättning med max 20 miljoner euro).

– I och med GDPR kommer verksamheter vara tvungna att anställa ett dataskyddsombud som enbart arbetar med personuppgiftshantering, har ni någon sådan person idag eller kommer ni vara tvungna att utbilda någon/använda er av konsult?

– Hur ser ni på att myndigheter kommer att ha större skyldigheter till att ge ut information om vilka uppgifter som lagras till invånaren?

– GDPR kan ses som en internationell "jobbigare" version av PuL som möjligtvis kommer ge er mer arbete än tidigare. Vad tycker ni om detta? Ser ni någon fördel med de extra arbetsmoment GDPR för med sig?

3 Sårbarhetsanalys.

– Vi vet att en risk och sårbarhetsanalys behöver göras för offentliga verksamheter vid införskaffande av tillexempel molntjänster, upprättade ni en sådan? Hur gick arbetet till?

– Var det någonting i risk och sårbarhetsanalys som öppnade upp era ögon för ett problem som ni tidigare inte tänkt på?

– Är det något som skiljer sig i arbetet med en sårbarhetsanalys för molntjänster jämfört med arbetet för en vanlig risk och sårbarhetsanalys?