LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Tillmötesgåendet av GDPR

Utmaningar ur ett tekniskt och processorienterat perspektiv

Kandidatuppsats 15 hp, **kurs SYSK02 i informationssystem och INFK11 i informatik**

Författare: Henrik Månsson
Joey Erichsen

Handledare: Odd Steen

Examinatorer: Magnus Wärja
Umberto Friccadori

Tillmötesgåendet av GDPR: Utmaningar ur ett teknisk och processorienterat perspektiv.

Författare: Henrik Månsson och Joey Erichsen

Utgivare: Inst. för informatik, Ekonomihögskolan, Lund universitet

Dokumenttyp: Kandidatuppsats

Antal sidor: 71

Nyckelord: GDPR, Privacy by Design, Processorienterad verksamhetsutveckling, Informationsteknik, Utmaningar.

Sammanfattning (Max. 200 ord):

Majoriteten av alla verksamheter idag lagrar personuppgifter i sina respektive informationssystem. Det är samtidigt inte ovanligt att det förekommer flera olika system, ibland upp emot tresiffrigt, för en och samma verksamhet. I april 2016 presenterades en ny dataskyddsförordning (GDPR) som kommer att träda i kraft i maj 2018, och vars syfte är att ge registrerade personer större kontroll över, och rättigheter till sina personuppgifter. Detta kommer att innebära en stor organisatorisk omställning för alla verksamheter med avseende på dess processer, men också deras tekniska system. Vår studie är ämnad att undersöka detta problemområde och identifiera vilka de största utmaningarna, rent tekniskt och processorienterat, för svenska verksamheter är. En kvalitativ undersökning har genomförts, vilken visar på att svenska verksamheter ställs inför snarlika utmaningar gällande själva omstruktureringsarbetet. Resultatet pekar framförallt på att själva kartläggningen och identifieringen av vad respektive system innehåller är bland de absolut största utmaningarna - alltså det förebyggande arbete för att sedan kunna genomföra processorienterade och tekniska förändringar. Vidare visar resultatet på att det kommer krävas nya verktyg och funktioner som automatiskt ska upptäcka incidenter, och därtill nya processer för att hantera varje enskild incident beroende på dess karaktär och omfattning.

Innehåll

1 Introduktion

1.1 Bakgrund

I takt med att olika verksamheters datasystem runt om i världen sedan en tid tillbaka och framåt har digitaliserats i allt större utsträckning, så har också mängden elektronisk data och information ökat. En betydande del utav denna information och data som lagras är personuppgifter om dels anställda, men också om verksamheters respektive kunder och användare. Den 27 april 2016 utfärdade Europaparlamentet att en ny dataskyddsförordning kommer att verkställas för samtliga medlemsstater i EU (Allmän dataskyddsförordning 2016/679 av den 27 april 2016). Dataskyddsförordningen kallas för "General Data Protection Regulation" (förkortat GDPR), och kommer att ersätta EU:s gamla dataskyddsdirektiv, 1995/46/EG (Allmän dataskyddsförordning 2016/679 av den 27 april 2016), och därmed den svenska personuppgiftslagen, PuL, från 1998 (Datainspektionen, 2017a). Med andra ord kommer GDPR tillämpas direkt utan vidare krav av lagstiftning för respektive medlemsstat inom EU - detta, den 25 maj 2018. (Datainspektionen, 2017a; Allmän dataskyddsförordning 2016/679 av den 27 april 2016).

GDPR kommer ställa betydligt högre krav på hur företag och organisationer samlar in personuppgifter om medborgare inom EU, samt hur personuppgifterna hanteras inom verksamheten. Det har ingen betydelse var verksamheten är beläget eller var personuppgifterna lagras någonstans, utan all personlig information om EU-medborgare kommer att regleras av GDPR. Till detta räknas allt som kan identifiera en enskild person, vilket även innebär att indirekt information, såsom IP-adresser och cookies, också kategoriseras som en personuppgift (Tankard, 2016). Vid överträdelse kan en verksamhet bli skyldig att betala en sanktion upp till 20 miljoner euro, eller upp till 4% av den globala årsomsättningen under föregående budgetår (Allmän dataskyddsförordning 2016/679 av den 27 april 2016).

Personer som är registrerade i en verksamhet kommer få en ökad rättighet till sina utelämnade personuppgifter. Detta innebär huvudsakligen rätten till att få tillgång till sina personuppgifter, men också få felaktiga personuppgifter rättade eller raderade. Vidare kommer den registrerade kunna invända mot att personuppgifterna används för direktmarknadsföring, eller för automatiserat beslutsfattande och profilering. Dessutom ger GDPR registrerade rättighet till att migrera sina personuppgifter (dataportabilitet), vilket innebär att vederbörande kan kräva att få sina personuppgifter flyttade från en organisation till en annan (Datainspektionen, 2017b). Därmed kommer GDPR innebära stora organisatoriska förändringar på rutiner, processer och särskilda administrativa ansvarsposter. Samtidigt ställs det högre tekniska krav gällande hantering av information som kan kopplas till en personuppgift.

1.2 Problemområde

Att arbeta mot ett tillmötesgående av GDPR är en tuff utmaning som förutsätter en mängd noga genomtänkta organisatoriska förändringar för en verksamhet att lösa. Detta därför att bestämmelser gällande GDPR deklarerar en rapporteringsskyldighet hos alla myndigheter, företag och organisationer vid en så kallad personuppgiftsincident. En personuppgiftsincident kan enligt definition vara ett dataintrång som leder till läckta personuppgifter, eller att en obehörig får tillgång till en verksamhets hanterade personuppgifter. Men det kan också vara att registrerade individers personuppgifter, utan begäran eller intention, förloras eller ändras (Datainspektionen, 2017b). Sådana incidenter ska enligt bestämmelser rapporteras av en personuppgiftsansvarig (det vill säga av den verksamhet som incidenten inträffat hos) till respektive medlemsstats tillsynsmyndighet (i svenska fall Datainspektionen) inom 72 timmar (Allmän dataskyddsförordning 2016/679 av den 27 april 2016). Det råder också en skyldighet för en anlitad personuppgiftsbiträde att informera den personuppgiftsansvarige att en säkerhetsincident har inträffat (Datainspektionen, 2017c). Till följd av denna nya rapporteringsskyldighet så ställs det därför nya utmaningar av en verksamhets processer, rutiner och policys - vilka således behöver att ses över och omstruktureras. Med detta tillkommer också tydliga ramverk för olika ansvarsposter för att kunna upptäcka, rapportera och sedan behandla en specifik personuppgiftsincident (Datainspektionen, 2017d). Vidare blir det upp till respektive verksamhet att redogöra för vilken grad av automatiserat systemstöd, samt omfattning av processer som denne måste tillämpa för att hantera en sådan incident.

Dataskyddsförordningen deklarerar inga specifika tekniska krav för verksamheters system. Däremot kommer det indirekt krävas att de olika systemen inom en och samma verksamhet är mer integrerade med varandra. Detta dels på grund av säkerhetsaspekter, det vill säga att det är nödvändigt att kunna betrakta systemen ur ett enhetligt och övergripande perspektiv. Vidare är det inte ovanligt att personuppgifter för en och samma registrerad individ lagras på olika ställen (det vill säga på olika system) inom samma verksamhet. Därmed blir det en fråga om effektivisering när det exempelvis handlar om att, på begäran av en registrerad, ta bort dennes personuppgifter till följd av GDPR's bestämmelse om rätten till att bli raderad - även kallad "rätten att bli bortglömd" (Allmän dataskyddsförordning 2016/679 av den 27 april 2016).

Omställningstiden på 2 år, innan verksamheter behöver tillmötesgå de krav som GDPR ställer, kommer innebära stora omstruktureringar inom verksamheter på kort tid, vilket inte bara är tidskrävande utan också kommer kräva stora resurser. Många verksamheter är heller inte förberedda inför införandet av GDPR. En undersökning genomförd av Dimensional Research (Appendix 7.1: bild 1) om verksamheters förberedelsegrad, visar att 33% av svenska verksamheter anser sig redo inför GDPR medan 39% av svenska verksamheter inte anser sig redo. Resterande 28% inte är medvetna om sin förberedelsegrad inför GDPR.

1.3 Forskningsfråga

Forskningsfrågan är formulerad i syfte att identifiera de största utmaningarna som svenska verksamheter står inför gällande tillmötesgåendet mot GDPR. Forskningsfrågan kommer vidare att riktas till personer med betydelsefullt inflytande angående just omställningsarbetet ute bland verksamheterna. Intentionen är emellertid inte att den insamlade empirin ska representera respektive verksamhets officiella åsikt, utan snarare intervjupersonernas egna uppfattningar. Forskningsfrågan lyder enligt följande:

Vilka är de största tekniska och processorienterade utmaningarna inför GDPR?

1.4 Syfte

Studiens syfte är främst att redogöra för de största utmaningar som olika verksamheter anser sig själva stå inför gällande tillmötesgåendet av GDPR. Vidare syftar studien till att identifiera de åtgärder som en verksamhet därefter måste vidta för att kunna tillmötesgå kraven för GDPR. Detta med fokus på tekniska tillämpningar och funktioner, men också processorienterade förändringar av rutiner inom verksamheterna.

1.5 Avgränsning

Studiens ändamål avgränsar sig till att inte undersöka eller samla in empiri från företag eller organisationer utanför Sveriges gränser. Det finns heller ingen avsikt att undersöka skräddarsydda system- och processlösningar som företag erbjuder i ett “business-to-business”-syfte. Istället kommer studien kommer endast utgå ifrån att undersöka verksamheter som själva tar sig an utmaningen om att genomföra omstruktureringsarbetet av GDPR. Dessutom är det de definierade utmaningarna från personer med betydelsefullt inflytande för respektive verksamhets omställningsarbete mot GDPR som är av intresse - istället för verksamhetens officiella åsikt.

2 Litteraturgenomgång

I detta kapitel behandlas den litteratur som varit till grund för studiens forskningsfråga. Litteraturgenomgången mynnar sedan ut i ett teoretiskt ramverk, vilket sedan använts för att skapa intervjufrågorna. Kapitlet inleds med definitioner av vanligt förekommande begrepp som är återkommande i uppsatsen och övergår sedan till juridiska definitioner gällande ett data-subjekt. Därefter introduceras läsaren till de tekniska riktlinjer som GDPR presenterar för att ge denne en inblick i problemområdet. Slutligen presenteras en genomgång kring processorienterad verksamhetsutveckling för att ge läsaren en inblick angående denna aspekt.

2.1 Definitioner av vanligt förekommande begrepp

2.1.1 Personuppgiftsansvarig

Personuppgiftsansvarig definieras enligt personuppgiftslagen: "*Personuppgiftsansvarig är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter*." (3 § personuppgiftslagen). En personuppgiftsansvarig behandlar personuppgifter och bestämmer hur dessa uppgifter ska användas, oftast är en personuppgiftsansvarig en juridisk person eller en myndighet (Datainspektionen, 2017e).

2.1.2 Personuppgiftsbiträde

Personuppgiftsbiträde definieras enligt personuppgiftslagen: *"Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning."* (3 § personuppgiftslagen). Personuppgiftsbiträdet behandlar utifrån riktlinjer och bestämmelser personuppgifter för personuppgiftsansvariga. Personuppgiftsbiträdet kan vara en fysisk person, men det kan likväl vara en juridisk person. Om en juridisk person anlitas som personuppgiftsbiträde för en verksamhet måste ett skriftligt avtal upprättas (Datainspektionen, 2017f).

2.1.3 Dataskyddsombud

Ett dataskyddsombud ska dels kontrollera att GDPR följs och dels agera som en kontaktperson inom organisationen både mot de som är registrerade och mot tillsynsmyndigheten. Dataskyddsombudet kan vara anställd inom organisationen men det är även möjligt att ha ett utomstående dataskyddsombud som inte har någon koppling till organisationen (Datainspektionen, 2017g).

2.1.4 GDPR

GDPR står för 'General Data Protection Regulation' och är den engelska termen för den nya dataskyddsförordningen. I uppsatsen kommer endast akronymet "GDPR" att användas.

2.2 Data-subjekt

2.2.1 Definition av personuppgift:

Enligt Allmän dataskyddsförordning 2016/679 av den 27 april (2016) definieras en personuppgift som: ”*Varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.”*. Med andra ord definieras en personuppgift enligt allt som kan identifiera en fysiskt levande person både direkt och indirekt genom GDPR. Detta gäller även bilder, ljudupptagningar, cookies och IP-adresser om de kan kopplas till en fysisk levande person.

2.2.2 De registrerades rättigheter

GDPR kommer framförallt beröra hur personuppgifter hanteras och skyddas i verksamheter. De registrerades rättigheter kommer inte skilja sig särskilt mycket från idag och personuppgiftslagen, utan istället kommer de registrerades rättigheter framför allt att förstärkas (Datainspektionen, 2017h). Med GDPR kommer de registrerade få större tillgång till de uppgifter verksamheter tillhandahåller (Allmän dataskyddsförordning 2016/679 av den 27 april 2016). Verksamheter ska kunna tillgodose de registrerade med information när vederbörandes personuppgifter behandlas, men även när personuppgifterna samlas in eller om de registrerade begär att få ut sina personuppgifter. Personuppgiftsansvariga behöver även informera de registrerade ifall det sker någon form av dataintrång, eller risk som berör de registrerades personuppgifter (Datainspektionen, 2017j).

Som registrerad har man rätt att få felaktiga personuppgifter behandlade och möjlighet att komplettera ofullständiga personuppgifter(Allmän dataskyddsförordning 2016/679 av den 27 april 2016). Man har som registrerad även möjlighet att få sina personuppgifter raderade och personuppgiftsansvariga ska dessutom radera de personuppgifter som inte längre används till de ändamål som de samlades in för (Allmän dataskyddsförordning 2016/679 av den 27 april 2016).

Rätten till dataportabilitet är nytt i GDPR (Datainspektionen, 2017k). Med dataportabilitet har de registrerade rätt att överföra personuppgifter som den registrerade har tillhandahållit, från en personuppgiftsansvarig till en annan utan någon form av invändning. Överföringen av personuppgifterna ska ske direkt, när detta är tekniskt möjligt (Allmän dataskyddsförordning 2016/679 av den 27 april 2016).

Missbruksregeln som många företag använder sig av idag för ostrukturerat material, som personuppgifter i mail, på internet eller bara i ett dokument på datorn, kommer också ersättas av GDPR när denne träder i kraft. Missbruksregeln ger verksamheter möjlighet att använda sig av enklare regler för hur ostrukturerat material inom verksamheten får behandlas. De regler som GDPR ställer på hanteringen av personuppgifter kommer även gälla för allt ostrukturerat material som hanteras inom verksamheten (Datainspektionen, 2017i).

2.3 Systemriktlinjer

2.3.1 Vad förespråkar GDPR?

GDPR slår fast en del olika krav som ställs på den personuppgiftsansvarige och personuppgiftsbiträdet att vidta lämpliga åtgärder för att garantera en hög säkerhetsnivå. Detta sträcker sig till både organisatoriska och tekniska åtgärder, beroende på grad av risk och omfattning, gällande säkerhet för registrerades personuppgifter (Allmän dataskyddsförordning 2016/679 av den 27 april 2016). GDPR reglerar uttryckligen att bygga in dataskydd direkt i systemen enligt *"Privacy by Design",* som en åtgärd på dessa tekniska krav (Datainspektionen, 2017d). Att använda kryptering och pseudonymisering vid hantering av personuppgifter, är ett av dessa krav som GDPR ställer (Allmän dataskyddsförordning 2016/679 av den 27 april 2016). Vidare ska det finnas funktioner som kontinuerligt garanterar integritet, konfidentialitet, tillgänglighet och begränsningar för systemanvändningen vid behandling av personuppgifter (Allmän dataskyddsförordning 2016/679 av den 27 april 2016). GDPR förutsätter också att det finns processer som regelbundet undersöker och utvärderar verksamhetens tekniska och organisatoriska åtgärder som ska garantera behandlingen av säkerheten (Allmän dataskyddsförordning 2016/679 av den 27 april 2016). Om en verksamhet uppfyller dessa krav, så finns möjlighet att erhålla en godkänd certifiering som verifierar säkerheten och tillmötesgåendet av GDPR (Allmän dataskyddsförordning 2016/679 av den 27 april 2016).

Vid inträffandet av en teknisk, eller fysisk personuppgiftsincident ska personuppgiftsansvarige, inom en rimlig tid, återställa tillgängligheten och tillgången till de berörda personuppgifterna (Allmän dataskyddsförordning 2016/679 av den 27 april 2016). Detta gäller emellertid endast incidenter som, av sannolika skäl, kan innebära en risk för de registrerades rättigheter gällande när deras personuppgifter kränks (Allmän dataskyddsförordning 2016/679 av den 27 april 2016). GDPR kräver att en personuppgiftsincident rapporteras av den personuppgiftsansvarige till tillsynsmyndigheten inom 72 timmar efter att incidenten upptäckts (Allmän dataskyddsförordning 2016/679 av den 27 april 2016). En sådan rapport ska bland annat innehålla specifikationer gällande incidentens art, samt det ungefärliga antalet registrerade personer som berörs av den. Slutligen ska rapporten beskriva de sannolika konsekvenser av gällande incident, men också de åtgärder

som personuppgiftsansvarige vidtagit för att förhindra eller förmildra incidentens negativa effekter (Allmän dataskyddsförordning 2016/679 av den 27 april 2016).

2.3.2 Certifiering

Med den nya förordningen kommer även införandet av certifieringsmekanismer för dataskydd med sigill och märkningar för dataskydd. Detta för att verksamheter ska kunna visa att deras personuppgiftsbehandling är förenlig med den nya förordningen. (Allmän dataskyddsförordning 2016/679 av den 27 april 2016). Rodrigues, R, Wright, D, & Wadhwa, K. (2013) definierar ”privacy seal” som en märkning av ett certifikat eller en garanti utfärdat av en certifierad enhet för att frambringa förtroende av en verksamhet. Certifieringen för GDPR är framtagen för att öka förståelsen av de krav som den nya förordningen ställer samt för att snabbt och enkelt kunna avgöra vilka typer av dataskydd, produkter och tjänster tillmötesgår (Rodrigues, R, Barnard-Wills, D, De Hert, P, & Papakonstantinou, V. 2016).

Verksamheter har möjlighet att tilldelas certifieringar för behandling av personuppgifter som är i enlighet med GDPR. För att tilldelas denna certifiering krävs att personuppgiftsansvarige eller personuppgiftsbiträdet har genomfört lämpliga tekniska och organisatoriska åtgärder såsom pseudonymisering och uppgiftsminimering, för att skydda de registrerades rättigheter. De personuppgifter som lagras ska endast vara de som är nödvändiga för ett specifikt ändamål. För detta gäller mängden insamlade uppgifter, behandlingens omfattning, tiden uppgifterna lagras samt tillgängligheten av personuppgifterna (Allmän dataskyddsförordning 2016/679 av den 27 april 2016).

Utförandet och förnyelsen av verksamheters certifiering utförs av den behöriga tillsynsmyndigheten eller av de certifieringsorgan som har lämplig nivå av expertis i form av dataskydd, och som har blivit ackrediterade av antingen den tillsynsmyndighet eller av det nationella ackrediteringsorgan som har blivit utsett av Europaparlamentets och rådets förordning, eller av båda två. Certifieringen gäller för högst tre år och kan därefter förnyas om de krav som certifieringen erfordrar fortsätter att uppfyllas. Skulle de krav som certifieringen ställer inte efterlevas, kan certifieringen återkallas och inte tilldelas igen förrän kraven uppfylls (Allmän dataskyddsförordning 2016/679 av den 27 april 2016).

2.3.3 Privacy by Design

Privacy by Design är ett förhållningssätt, eller ett ramverk inom systemutveckling vars fundamentala ändamål syftar till att informationssystem och organisationer ska sträva efter att tillhandahålla så lite information av kategorin “personuppgifter” som möjligt (Freytag, J C. Kargl, F. Kung, A. 2011). Detta innebär i sin tur att personuppgifter som saknar relevans för ett aktuellt syfte, inte heller ska samlas in. Vidare handlar det om att ta bort personuppgifter som inte längre används för något specifikt ändamål, men som trots detta fortfarande ligger sparat i systemet (Schaar, P. 2010). Att förhålla sig till Privacy by Design innebär emellertid

inte endast ett speciellt tankesätt, eller en viss praxis som appliceras till användandet av ett informationssystem. Det ska snarare ses som en säkerhetsåtgärd som är inbyggt i själva systemarkitekturen, och som redan från ett konceptuellt planeringsstadie tas i beaktning av utvecklare och projektledare (Diaz, C. Gürses, S. Troncoso, C. 2011). Dessutom ska det genomsyra informationssystemet hela vägen fram till implementering och användning (Schaar, P. 2010).

Ramverket bygger främst på principen "data minimization", eller data-minimering, vilket innebär att endast nödvändig och aktuell information om en registrerad person ska lagras i ett system (Schaar, P. 2010; Diaz, C. Gürses, S. Troncoso, C. 2011). Men Privacy by Design hänvisar inte enbart till att implementeras för IT-system. Cavoukian, A (2010) menar att Privacy by Design också kan appliceras som en verksamhetspraxis, likväl som inom fysisk design och infrastruktur. Vidare beskrivs det att Privacy by Design uppnås genom att fokusera på att eftersträva 7 grundläggande principer (Cavoukian, A. 2010);

1. *Proaktiv istället för reaktiv; Förebyggande istället för åtgärdande.*
   Privacy by Design ska inte ses som ett verktyg för att åtgärda ett inträffande problem, istället ämnar det till att förebygga problem från att inträffa. Detta genom att anta en proaktiv inställning inför eventuella framtida problem, istället för en reaktiv åtgärd efter att de redan inträffat (Cavoukian, A. 2010).

2. *Identitetsskydd som standard (Privacy as the Default).*
   Privacy by Design strävar efter att nå maximal nivå av identitetsskydd genom att personuppgifter skyddas via automatiserade processer för IT-system och inom verksamhetspraxis. Inga manuella åtgärder ska krävas från personuppgiftsansvariges sida för att garantera hög säkerhet, liksom ingen åtgärd från den registrerades sida ska behöva göras för att dennes personuppgifter ska förbli väl skyddat. Med andra ord är identitetsskyddet inbyggt som standard i systemen (Cavoukian, A. 2010).

3. *Identitetsskydd invävt i designen.*
   Identitetsskydd får inte vara en extern komponent eller applikation som appliceras till ett system eller verksamhet. Privacy by Design förespråkar istället att väva in identitetsskyddet och säkerheten i system- och verksamhetsarkitekturen. På så sätt blir detta skydd en del av systemets eller verksamhetens essentiella grundpelare och finns integrerat från början, samt utan brister i funktionaliteten (Cavoukian, A. 2010).

4. *Full funktionalitet - utan avvägningar.*
   Till skillnad från nollsummeringsprincipen (zero-sum), vilken deklarerar att allt har en alternativkostnad som en konsekvens av ett visst val, så utgår Privacy by Design från principen om att en summering med ett positivt utfall är möjlig. Detta innebär exempelvis att säkerhet inte ska vägas mot integritet i ett "antingen/eller-scenario". Istället strävar Privacy by Design mot att full funktionalitet är möjligt, och därmed uppnås genom att tillämpa både säkerhet och integritet i ett "win-win-scenario"

(Cavoukian, A. 2010).

5. *Säkerhet genom hela data-livscykeln.*
   Genom att väva in identitetsskydd i hela system- och verksamhetsarkitekturen, så garanteras data vara skyddad genom hela dess livscykel - från insamling av data tills dess att den inte längre behövs. Detta ska också säkerställa att berörd data förstörs efter den tidpunkt då datan inte längre används för ett specifikt syfte (Cavoukian, A. 2010).

6. *Synlighet och transparens.*
   Privacy by Design förespråkar att en personuppgiftsansvarig ska kunna försäkra alla involverade parter om att denne, enligt angivna löften, följer de avtalade regler och riktlinjer som avtalats. Detta genom transparens hos den personuppgiftsansvarige gentemot registrerade och leverantörer, så att ett förtroende mellan dem kan etableras (Cavoukian, A. 2010).

7. *Respekt för användarnas integritet.*
   En av de mest essentiella förutsättningarna för Privacy by Design är att personuppgiftsansvarige prioriterar den registrerades behov av ett system. Till detta hör främst starka villkor för identitetsskydd, men också användarcentrerade operationer som förbättrar prestandan av systemet till en mer användarvänlig miljö (Cavoukian, A. 2010).

Liksom första principen deklarerar, så utgår Privacy by Design inte från att att åtgärda en upptäckt incident i ett system eller en verksamhet. Därmed ska inte Privacy by Design inte ses som ett verktyg, eller riktlinje för att lösa ett aktuellt problem. Istället visar Cavoukian's ovanstående 7 principer på hur en verksamhet, på ett konceptuellt stadie, kan anta en proaktiv strategi för att i förebyggande syfte mitigera vanliga säkerhetsrisker gällande registrerades integritet.

2.4 Verksamhetsförändringar

2.4.1 Business Process Reengineering

Hammer, Champy, & Svensson (1994, s.40) definierar reengineering enligt:
"*Ett fundamentalt nytänkande och en radikal förändring av verksamhetsprocesserna i syfte att nå dramatiska förändringar vad avser viktiga, moderna effektivitetsmått som kostnader, kvalitet, service och snabbhet.*"

Business Process Reengineering, hädanefter BPR, grundar sig i, att istället för att stegvis förbättra processerna, bryta ner processerna helt och börja om från början. Att överge

etablerade processer och utveckla nya, möjliggör ett nytt tänkande och ett nytt fokus över hur de nya processerna bör utvecklas (Hammer, M, Champy, J, & Svensson, P. 1994). Vid omstrukturering menar Hammer, Champy, & Svensson (1994) att det är logiskt att dela upp anställda i särskilda processteam för att driva en hel process för att ersätta organisationen med avdelningar. Hammer, Champy, & Svensson (1994) belyser vikten av fyra nyckelord i definitionen av BPR: Fundamental, radikal, dramatisk och processer.

Med fundamental menar Hammer, Champy, & Svensson (1994) att företagsledningen måste förstå hur och varför företaget väljer att arbeta på det sätt som de gör. Genom att besvara de mest elementära frågorna bildar man sig en tydligare överblick om hur företaget faktiskt styr deras sätt att arbeta och ofta visar det sig att delar av arbetsprocesserna är föråldrade eller felaktiga. Med *radikal* menar Hammer, Champy, & Svensson (1994) att man måste göra radikala förändringar för att uppnå effekt. Genom att bortse från befintlig struktur och procedurer och istället fokusera på roten av problemet, utveckla nya sätt att arbeta på. Med *dramatisk* menar Hammer, Champy, & Svensson (1994) att reengineering kräver dramatiska förändringar för att ge effekt. Det handlar inte om små marginella förbättringar utan reengineering kräver att man ersätter det gamla med nytt. Hammer, Champy, & Svensson (1994) framhäver processer som det viktigaste ordet i definitionen av BPR. De menar att de flesta ledare inte är processorienterade utan istället fokuserar på enskilda arbetsmoment eller uppgifter istället för processen som helhet.

Att utveckla en ny process genom reengineering kräver en del kreativitet, det finns till exempel inga tillvägagångssätt för hur man ska göra eller eventuella steg att följa (Hammer, M, Champy, J, & Svensson, P.1994). Hammer, Champy, & Svensson (1994) framhäver betydelsen av att ta del av hur andra företag har lyckats med sina reengineerade processer och identifiera de återkommande mönster som frambringar lyckade processförändringar. Hammer, Hammer, Champy, & Svensson (1994) uppskattar att 50-70% av företag misslyckas med uppnå ett framgångsrikt resultat men understryker trots den höga siffran att reengineering inte är ett högriskprojekt utan att det istället handlar om att vara medveten om vanliga fel vid misslyckanden och undvika dem.

2.4.2 Change Management ur ett ledarperspektiv

Moran och Brightman (2001) definierar Change Management enligt en process av kontinuerligt förnyande av en organisations riktning, struktur samt förmågor i syfte att tjäna det föränderliga behovet av dels externa, men också interna faktorer. Det finns emellertid inget allmänt och praktiskt tillvägagångssätt för hur Change Management ska tillämpas i en verksamhet, utan istället har olika ramverk eller förhållningssätt utformats för att anta en omstrukturering utifrån olika aspekter (Todnem By, R. 2007). Detta kan delvis förklaras genom att verksamheter sinsemellan ser väldigt olika ut. Men också att olika verksamheters behov samt anledning till en viss förändring varierar; exempelvis kan en förändring vara en konsekvens av att ny teknologi introduceras, konkurrens, men också en funktion av att nya lagar inrättas (Paton, R A. McCalman, J. 2000).

Moran och Brightman (2001) förklarar hur Change Management kan appliceras till ledarrollen för ett förändringsarbete inom en verksamhet. Vidare beskriver de ett arbetssätt utifrån en processcykel, varvid fyra stycken faser ständigt ska itereras. Den inledande fasen syftar till att förstå den rådande situationen. Med detta tillkommer att en person, i egenskap av ledare för förändringsarbetet, måste förstå orsaken till varför en förändring är nödvändig, men samtidigt ha i åtanke att förändringen ska vara i enlighet med verksamhetens strategiska affärsmål (Moran, J W. Brightman, B K. 2001). Därmed måste det finnas en god insyn om vad de rådande omständigheterna kan orsaka för konsekvenser för verksamheten ifall en förändring inte sker. Kommunikation inom verksamheten och med olika intressenter är därför också en viktig aktivitet för att förstå omfattningen av processer och personer som berörs av förändringen (Moran, J W. Brightman, B K. 2001).

Fas två handlar om att utveckla en förändringsplan utifrån det önskade målet av förändringen. Moran och Brightman (2001) betonar att en sådan plan inte enbart ska utformas utifrån ett perspektiv. Internt inom verksamheten, likväl som externt bland intressenter uppenbarar sig sannolikt många olika förslag och prioriteringar för hur en förändring ska ske, varpå kommunikation återigen blir en kritisk utgångspunkt. Vidare finns det alltid en viss nivå av risk att en förändring bemöts av motstånd hos anställda som gör att förändringsarbetet kan bli ineffektivt (Paton, R A. McCalman, J 2000). Patron och McCalman (2000) pekar då också på att kommunikation och informering är de främsta nyckelaktiviteterna för att mitigera detta motstånd. Detta med tanke på att den vanligaste orsaken till motstånd grundar sig i rädslan för det okända (Paton, R A. McCalman, J 2000: Moran, J W. Brightman, B K. 2001).

Efterhand som omfattningen av förändringen upptäcks och utvärderas, måste fler och fler personer involveras i arbetet (Moran, J W. Brightman, B K. 2001). Fas tre syftar därmed till att bredda kompetensen inom förändringsarbetet till att fler blir involverade, och att de i sin tur besitter djupare insikt angående intentionerna samt målen med förändringen. Detta bidrar också till att nya infallsvinklar och perspektiv diskuteras fram, och vilka sedan kan utvärderas så att allmän större förståelse i verksamheten kan uppnås (Moran, J W. Brightman, B K. 2001). Moran och Brightman (2001) argumenterar även för en så kallad “kritisk massa” som måste underrättas för att dels motståndsfaktorn ska förebyggas, men också att varje individ i verksamheten ska vara tillräckligt införstådda med förändringen att de aktivt och självständigt kan arbeta för att bidra till effektiviseringen av hela projektet.

Den fjärde och sista fasen i processcykeln syftar till att identifiera och stabilisera resultat (Moran, J W. Brightman, B K. 2001). Genom att konsekvent mäta olika resultat av förändringsarbetet skapas en insikt om hur väl verksamheten arbetar i förhållande till de utsatta målen. Det blir på så sätt enklare att greppa arbetets helhet på en individnivå för alla enskilda anställda, vilket dessutom kan öka motivationen. Denna motivation kan även stärkas genom att tydligt redovisa för verksamheten när olika delmål har uppfyllts (Moran, J W. Brightman, B K. 2001).

2.5 Teoretiskt ramverk

Kategori	Litteratur	Undersöker
Data-subjekt	**Allmän dataskyddsförordning 2016/679 av den 27 april 2016**	- Definition av personuppgift - Registrerades rättigheter
Systemriktlinjer	**Privacy by Design** (Freytag, J C. Kargl, F. Kung, A. 2011), (Schaar, P. 2010), (Diaz, C. Gürses, S. Troncoso, C. 2011), (Cavoukian, A. 2010). **Implementering av Privacy by Design** (Diaz, C. Gürses, S. Troncoso, C. 2011), (Cavoukian, A. 2010). **Allmän dataskyddsförordning 2016/679 av den 27 april 2016**	- Säkerhet integrerat i informationssystem. - Data-minimering - Utmaningar med implementering av Privacy by Design - Möjligheten till GDPR-certifiering
Verksamhetsförändringar	**Business Process Reengineering** (Hammer, M. Champy, J. 1994) **Change Management** (Paton, R A. McCalman, J. 2000), (Todnem By, Rune. 2007). **Ledning vid en organisatorisk förändring** (Moran, J W. Brightman, B K. 2001).	- Processrevidering - Konsekvenser, samt utmaningar med Change Management - Mitigering av konsekvenser vid organisationsför-ändringar ur ett ledarperspektiv

Tabell 1: Teoretiskt Ramverk

3 Metod

I detta kapitel förklaras den vetenskapliga metod och tillvägagångssätt som studien är utförd enligt för att forskningsfrågan ska kunna besvaras. Vidare presenteras de metodval som utförts, hur urvalsprocessen gått till, vilken intervjustruktur som använts samt hur transkribering och analys av intervjusvaren har processerats. Dessutom innehåller kapitlet en genomgång över undersökningskvaliteten som ligger till grund för hur studien har utformats, och utifrån vilka aspekter som har tagits i beaktning för att studien ska hålla hög kvalitet och så få felfaktorer som möjligt.

3.1 Insamling av empirisk data

3.1.1 Metodval

Det finns två olika metodologier vid insamling av empirisk forskningsdata. Dessa är kvalitativa, respektive kvantitativa studier (Jacobsen, 2002). Tillvägagångssättet för en kvalitativ studie innebär att undersökaren samlar data från en handfull olika respondenter i samband med intervjuer (Jacobsen, 2002). Vid en kvalitativ studie möjliggörs en mer detaljerad data att analysera då öppet samtal mellan respondent och undersökare ger större utrymme och djup kring problembeskrivningen (Jacobsen, 2002). Kvantitativa studier å andra sidan erbjuder en mer generaliserad analys av datan då enkäter vanligtvis delas ut till ett betydligt större antal respondenter, samt med fördefinierade svarsalternativ. Detta resulterar emellertid i ett snävare spektrum av detaljerad data med tanke på att ingen vidare motivering av svaren kan erbjudas (Jacobsen, 2002).

I vår studie har vi med avsikt valt att tillämpa en kvalitativ metodologi då vi söker efter djupare och mer nyanserad data från respondenterna. Därför har vi också identifierat ett fåtal nyckelpersoner från olika verksamheter och branscher som innehar en betydande roll för respektive områdes omställningsarbete i tillmötesgåendet av GDPR, vilka vi sedan intervjuat. Alla respondenter har i grunden fått samma frågor och finns sammanställda i Tabell 2: Intervjupersoner. Men beroende på deras respektive svar så har vidare frågor spontant, dock med tydlig relevans, ställts för att få en mer utökad och detaljerad beskrivning av vad de menar. Frågorna är vidare definierade utifrån vårt teoretiska ramverk som i sin tur är en funktion av vår teori och forskningsfråga, samt återfinns i Appendix 7.2: Intervjufrågor.

3.1.2 Urval

Vår urvalsprocess har utgått ifrån att tillfråga personer med så stort inflytande i en verksamhets omställningsarbete gällande GDPR. Detta för att på det mest optimala sättet lyckas samla in så kvalitativ data, och från personer med så bred kompetens inom ämnet, som möjligt. I detta avseendet så har därmed den efterfrågade kompetensen utgått från erfarenheter

inom dels juridiska, datasäkerhetsmässiga, men också projektledningsmässiga aspekter. Respondenterna som vi intervjuat har olika erfarenheter inom arbetslivet då somliga tidigare arbetat som jurister, medan andra som säkerhetsspecialister för diverse informationssystems-projekt. Gemensamt för dem alla är dock, och som tidigare nämnt, att de besitter en betydande roll för respektive verksamhets aktuella omställningsarbete i tillmötesgåendet av GDPR.

Vi inledde en e-postkonversation med samtliga företag i Tabell 2, där vi först presenterade oss och vårt syfte, och sedan ställde frågan ifall de hade en egen intern grupp som arbetade med tillmötesgåendet av GDPR. Vidare förklarade att vi efterfrågade en intervju med en anställd från deras företag och ifall det fanns en möjlighet till detta. Vi förklarade samtidigt att vi ansåg det vara mest lämpligt att respektive företag vidarekopplade oss till en anställd som de själva tyckte var bäst kvalificerad för den intervju vi efterfrågade. Detta för att de torde ha bäst insikt i sin egna organisation om vilken person som var den lämpligaste respondenten. Utfallet av våra e-postutskick visade sig vara mycket bra, och resulterade i intervjuer med samtliga tillfrågade företag - E.ON, LDC, Företag X och Företag Y.

Person	Namn	Företag	Position	Plats	Intervjutyp	Appendix
IP1	Ola Alsén	E.ON	Personuppgiftsombud	Malmö	Möte	Appendix 8.1.1
IP2	Magnus Persson	LDC	IT-säkerhetsarkitekt	Lund	Möte	Appendix 8.1.2
IP3	Michael Lindström	Företag X	Informationssäkerhetschef	Helsingborg	Möte	Appendix 8.1.3
IP4	Magnus Svensson	Företag Y	Projektledare för GDPR-omställning.	Helsingborg	Möte	Appendix 8.1.4

Tabell 2: Intervjupersoner

3.2 Intervjustruktur

Intervjufrågorna vi ställde till respondenterna var av strukturerad karaktär, vilket innebär att vi hade förbestämda teman och frågor att ställa till samtliga av dem. Däremot var strukturen till den grad av öppenhet att svaren från respondenten presenterades muntligt utan att vi gav dem några fördefinierade svarsalternativ. Även om alla frågor var förbestämda, så lämnade vi emellertid utrymme för ge respondenterna följdfrågor på eventuella svar som vi ville att de skulle utveckla, eller förklara närmare i detalj. Det kunde också te sig på det sättet att vi helt enkelt inte förstod hela innebörden av ett svar från respondenten, varpå vi bad dem att förklara med ett exempel eller försöka presentera det mer begripligt.

GDPR är en lag som innefattar ett brett ämne och ett stort urval av tolkningar för olika verksamheter. Detta med tanke på att verksamheter ser olika ut å ena sidan rent organisationsmässigt, men också sett till dess omfattning av systemanvändning, vilket också lämnar ett brett spektrum av nyansering för respondenternas svar. För att undvika detta - och därigenom mitigera ett annars komplext, samt resurskrävande analysarbete - så valde vi att begränsa och konkretisera våra intervjufrågor utefter vårt teoretiska ramverk. Syftet med denna strategi var att säkerställa att respondenternas svar också skulle vara relevanta för vår forskningsfråga, och därmed hela vår studie.

Varje intervju inleddes med att fråga respondenterna ifall de godkände att intervjun spelades in. Syftet till att vi hade för avsikt att spela intervjuerna var för att respektive respondents svar skulle bli enklare att transkribera, samt analysera i efterhand. Därefter klargjordes det för respondenterna att de hade rätt till att vara anonym i samband med vår studie om så önskades. Intervjufrågorna delades in enligt en tematisk modell, med inledande och övergripande frågor. Frågorna kategoriserades sedan efter först tekniska aspekter, och sedan efter processorienterade och organisatoriska aspekter. Avslutningsvis fick samtliga respondenter frågor gällande deras syn och åsikt om saker som GDPR förespråkar - exempelvis “Privacy by Design” och diverse certifieringsmekanismer.

De inledande frågorna som ställdes berörde vilka bakgrunder av studier, samt tidigare arbetslivserfarenheter som respondenterna hade. Dessutom frågade vi efter vilken roll som respondenterna hade på respektive företag. Vidare segment av frågeställningar handlade om hur stor omfattning respondenternas respektive förändringsarbete i tillmötesgåendet mot GDPR innefattar; det vill säga, hur många system som berörs samt hur många personer som ingår i projektet. Efterföljande frågor sökte efter att identifiera de största utmaningarna med tillmötesgåendet, dels tekniskt, men också process- och organisationsmässigt.

3.3 Transkribering och analys av intervjusvar

Som utgångspunkt bestämde vi att allt inspelat material skulle redovisas i transkriberingen ordagrant, med undantag från otydliga och oförståeliga ord eller otydligt tal. Icke relevanta frågor eller påståenden som uppkom under intervjun togs bort. Likaså transkriberades de tilläggs- och diskussionsfrågor som uppkom utifrån svar från huvudfrågorna och som var relevanta till resultatet och analysen av uppsatsen.

Varje intervjuperson tillfrågades innan intervju om anonymitet och en av intervjupersonerna ville först godkänna transkriberingen av intervjun innan denne svarade på frågan om anonymitet. På begäran av Michael Lindström, så har vi pseudonymiserat verksamheten han arbetar på. Denna verksamhet kommer därmed att omnämnas “Företag X” för att det riktiga verksamhetsnamnet inte ska kunna utläsas i uppsatsen. Det samma gäller för Magnus Svenssons företag, vilket vi således pseudonymiserat och omnämns därefter under namnet

"Företag Y". Ingen av dem hade emellertid några önskemål om att personligen vara anonyma, varpå deras namn fortfarande är korrekt återgivna. Utgångsfrågorna är markerade i transkriberingen med fet text för att få bättre förståelse om ämnet studien berör. Vanlig text i transkriberingen är antingen svar på en fråga, en tilläggsfråga eller bara ett påstående och är markerat utifrån vem som för samtalet.

För att lättare analysera och diskutera resultatet av intervjuerna sammanfattades all transkribering av respektive intervjuperson, detta för att få en tydligare överblick över varje intervjupersons respektive svar. Varje fråga, svar eller påstående har även numreras utifrån intervju för att lättare referera till, vid resultat och analys.

3.4 Undersökningskvalitet

3.4.1 Validitet och reliabilitet

Jacobsen (2002) definierar framför allt två olika former av validitet gällande en studie; Intern, respektive extern validitet. Den interna validiteten beskrivs enligt hur pass trovärdig resultatet av den insamlade empirin är, medan den externa validiteten syftar till hur pass representativ, eller generaliserbar resultatet är (Jacobsen, 2002). Ett sätt att stärka studiens inre validitet, vilket vi dessutom har tillämpat, är att i efterhand skicka transkriberingen från intervjuerna till respektive respondent. Detta för att säkerställa att transkriberingen är korrekt gjord och överensstämmer med respondenternas respektive hållpunkt, samt att inget missförstånd har skett. Det öppnar därmed också en möjlighet för en respondent att korrigera eventuella felaktigheter, vilka sedan kan åtgärdas.

Reliabiliteten i en studie syftar till hur tillförlitlig eller trovärdig den insamlade empirin är (Jacobsen, 2002). Vidare förklarar Jacobsen (2002) olika kontexteffekter som kan påverka reliabiliteten av en undersökning. Huruvida kontexten av en undersökning är naturlig eller artificiell visar sig kunna påverka intervjuobjektet rent psykologiskt (Jacobsen, 2002). En naturlig kontext innebär att intervjun sker på en plats som för intervjuobjektet är bekant och naturlig i sin miljö; exempelvis på dennes kontor (Jacobsen, 2002). En artificiell kontext innebär, tvärtom, att intervjun försiggår på en plats som för intervjuobjektet är obekant eller direkt olämplig för undersökningens syfte; exempelvis på en plats som intervjuobjektet tidigare aldrig besökt (Jacobsen, 2002). I samband med våra undersökningar har samtliga intervjuer ägt rum på respektive respondents arbetsplats. Detta dels för att undvika eventuella störningsmoment som annars skulle kunna uppstå genom att hålla intervjun på en tidigare okänd plats för dem. Men vårt val av intervjuplats grundar sig också på en tidsaspekt; det vill säga att uppta så lite arbetstid som möjligt för de intervjuade personerna, och därmed inte orsaka onödig stress för dem som eventuellt skulle kunna uppstå ifall de avsatte för mycket arbetstid på intervjun.

Jacobsen (2002) påpekar dessutom en annan dimension av kontexteffekter - nämligen ifall intervjun sker planerad eller överraskande. Detta syftar till ifall intervjuobjektet känner till att intervjun kommer äga rum i förväg eller ej. Vid en kvalitativ undersökning där djupare synpunkter och analyser av en fråga eftersträvas, så är en planlagd intervju det bästa alternativet då intervjuobjektet har haft en möjlighet till att kunna förbereda sig i förväg (Jacobsen, 2002). Därför har vi i samband med vår undersökning kontaktat respektive intervjuobjekt i förväg och därigenom avtalat en mötestid som passade båda parter.

3.4.2 Etik

Eftersom undersökningar alltid i någon mening inkräktar på en individs privata sfär, så är det viktigt att ta hänsyn till en mängd etiska aspekter. Jacobsen (2002) beskriver tre stycken etiska grundkrav som huvudsakligen bör tas i beaktning vid utförandet av en undersökning; *informerat samtycke, krav på privatliv* och *krav på att blir korrekt återgiven*.
Ett informerat samtycke definieras genom fyra krav, varvid den intervjuade personen först och främst ska besitta en tillräcklig *kompetens* om innebörden med att delta, och därmed vara förmögen att aktivt själv bestämma ifall han eller hon ska delta i en undersökning eller ej (Jacobsen, 2002). Vidare får det inte existera några kringliggande påtryckningar som kan påverka det aktiva valet hos intervjupersonen, vilket i sin tur medför att dennes deltagande inte är helt *frivilligt* (Jacobsen, 2002). Dessutom beskriver Jacobsen (2002) att den intervjuade personen ska vara tilldelad *full information* gällande undersökningens syfte, samt de eventuella konsekvenser som den vidare kan resultera i. Det kan emellertid innebära problem ifall den intervjuade personen har absolut full insikt i undersökningens syfte. Detta därför att reliabiliteten för svaren kan påverkas på ett negativt sätt eftersom den intervjuade personen då inte sällan anpassar sina svar efter just detta syfte (Jacobsen 2002). Slutligen menar Jacobsen (2002) att den intervjuade personen också måste ha *förståelse* för den information som presenteras, samt veta innebörden med de eventuella konsekvenser som undersökningen kan få.

Det andra etiska grundkravet enligt Jacobsen (2002) syftar till beaktning av den intervjuade personens privatliv. Till detta hör det att undersökarna tar hänsyn till vilka uppgifter som för den intervjuade personen kan vara känsliga, och därmed bör exkluderas i studien (Jacobsen 2002). Vilka uppgifter som räknas vara känsliga är emellertid högst individuellt, och ett sådant beslut bör därmed inte tas av undersökarna själva. Därför är det viktigt att den intervjuade personen blir tillfrågad om denne önskar vara anonym i samband med studien (Jacobsen 2002).

Det sista grundkravet som Jacobsen (2002) beskriver gällande etik, är att den intervjuade personen ska bli korrekt återgiven i samband med de svar som denne anger. Detta innebär främst att man som undersökare i största möjliga utsträckning ska återge resultatet från empirin så fullständigt, och i korrekt sammanhang som möjligt (Jacobsen 2002). Det kan tyckas självklart, men samtidigt menar Jacobsen (2002) att det inte alls är ovanligt att förfalskning och manipulation av resultat förekommer inom vetenskapliga undersökningar.

I bakgrund till dessa ovanstående faktorer, har vi vidtagit åtgärder för att försäkra de intervjuade personernas integritet; I samband med att vi tog kontakt med respondenterna, presenterade vi samtidigt studiens huvudsakliga syfte tillsammans med en kortfattad informationstext gällande vilka frågor vi bland annat intresserade oss för. Dessutom frågade vi respektive verksamhet att själva utse en bra lämpad kandidat till den tänkta intervjun. Varje intervjutillfälle inleddes också med att fråga respondenten ifall denne godkände att vi spelade in intervjun, och ifall han eller hon önskade att vara anonym i studien. Slutligen avslutades intervjuerna med att vi ställde frågan ifall respondenten önskade att ta del av vår transkribering för att säkerställa att denne ansåg sig ha blivit korrekt återgiven.

3.4.3 Plats

Varje intervju har genomförts på respektive respondents arbetsplats, ofta i något typ av konferensrum. Vid bestämmandet av plats har vi utgått helt ifrån vad som passar intervjuobjektet bäst. Detta dels för att det ska kännas mer naturligt för dem, men också för att underlätta med deras dagliga arbete. Med en naturlig plats menar Jacobsen (2002), en plats som intervjupersonen är välbekant med. Forskning har visat att miljön vid intervjun även påverkar själva resultatet (Jacobsen, 2002). Vidare förklarar Jacobsen (2002) att en onaturlig miljö kan frambringa svar som kan komma att påverka tillförlitligheten.

För att få en mer naturlig samtalskontakt med intervjuobjekten valde vi att använda oss av inspelningsutrustning vid intervjuerna. Jacobsen (2002) förklarar att inspelningsutrustning ger ett mer flytande samtal samtidigt som möjligheten till att använda sig av ordagranna citat kan kan ge rapporten extra tyngd. Användandet av inspelningsutrustning har från våran del varit ett självklart val och ingen av intervjupersonerna har haft någon invändning mot det. Men visst finns det nackdelar med att använda sig inspelningsutrustning. Jacobsen (2002) menar att användningen av inspelningsutrustning kan göra det svårare för intervjuobjektet att bland annat slappna av.

4 Resultat

Följande kapitel presenterar resultatet av den kvalitativa empiriska studie som genomförts. Resultaten är sammanställda i en tabell med respektive respondents svar på intervjufrågorna. Strukturens syfte är att ge en så retorisk presentation av resultatet som möjligt så att läsaren på ett enkelt sätt ska kunna redogöra och urskilja varje respondents svar så tydligt som möjligt, och därefter lätt kunna jämföra respektive svar med varandra.

Fråga	IP1	IP2	IP3	IP4
Hur jobbar ni i verksamheten för att tillmötesgå GDPR?	Jobbar mycket med utbildningar för att få mer awareness. Stora och små utbildningar anpassade efter målgrupp. Till exempel mot HR-avdelning, ledningsgrupp och liknande.(IP1.16)	Universitetet som driver frågan om GDPR. Tvådelad utredning där första delen handlar om hur man ska göra rent organisatoriskt. Andra delen handlar om att faktiskt förändra system och processer.(IP2.10; IP2.20)	Startade tidigt ett projekt som till en början gick ut på att försöka identifiera företagets nuvarande position. Efterhand som kunskapen om positionen vuxit så har man kunnat övergå till att fokusera på specifika åtgärder i nya delprojekt (IP3.14)	Ett GDPR-program startades, vilken leds av tre externa konsulter. Detta för att programmet ska kunna drivas med ett stort fokus utan att belasta befintliga arbetsposter på företaget (IP4.10).
Hur många består gruppen som bedriver förändringsarbetet?	Central projektgrupp i för hela Europa men för E.ON Sverige endast två stycken, två jurister som driver ett övergripande projekt.(IP1.26; IP1.32)	Beroende på vilket system som ska anpassas.(IP2.24)	Projektgruppen som aktivt arbetar med GDPR-frågan är cirka 15 stycken. Ledarna för projektet utgörs av externa konsulter. Efterhand som projektet fortlöper så inkluderas fler och fler i verksamheten (IP3. 16)	Projektgruppen består av cirka 15-20 stycken personer på olika arbetstimmar (IP4.26).

Hur stor omfattning är förändringsarbetet ? Hur många system berörs?	240-250 system på 10 bolag inom E.ON Sverige. 40-50 system om man räknar enskilda system. (IP1.36)	För LDC, kanske 5 system. Inte speciellt mycket persondata i systemen. System som har utvecklats till andra är säkert ett tiotal. (IP2.26)	X	189 stycken system berörs. Men omfattningen berör också olika enheter inom företaget. Varje enhet har i sin tur olika behandlingar av personuppgifter. Går man sen ner på individnivå så ökar omfattningen ytterligare. På så sätt är det svårt att definiera totala omfattningen - förutom att det är väldigt stort. (IP4.14; IP4.16).
Vilka är de största utmaningarna gällande tillmötesgåendet av GDPR, rent tekniskt?	Dataflödet, att säkerställa var alla personuppgifter finns och var de flödar och när de flyttas. (IP1.38; IP1.40)	Privacy by design.(IP2.28)	Investera i rätt tekniska verktyg som, automatiserat, upptäcker incidenter. Detta, tillsammans med bevisinsamling till en rapportering ur ett tidsperspektiv (IP3.22).	Data Breach, "Rätten att bli glömd" och pseudonymisering. Att se till att detta efterlevs i samtliga 189 system, känns väldigt svårt (IP4.18).
Hur ska ni göra för att tackla dessa tekniska utmaningar?	Helt olika lösningar beroende på system. Men försöker hålla all basdata i SAP som ett centralt system.(IP1.42)	För LDC handlar det om tid, pengar och resurser.(IP2.30)	Genom kartläggning av alla systemen så att det finns tillräckligt bra underlag för en investering i nya verktyg (IP3.24).	Genom att analysera varje system får vi en uppfattning om vilka förändringar de kräver, antingen tekniska, eller processorienterade. Men lösningarna går inte att lägga på varje enskilt system, utan måste ligga ovanför systemen som en generell tjänster och lösningar (IP4.20; IP4.22).

Vilka tekniska förändringar har ni förändrat eller planerar ni att förändra för att tillmötesgå de krav som GDPR ställer?	Beroende på applikation men rent generellt så är det att få till en loggning som fungerar så man har koll på alla uppgifter. Få till radering - gallringsrutiner, registerutdrag och att ha en systematik som är bättre sammankopplat till SAP. (IP1.44)	Inga tekniska förändringar än.(IP2.34)	Har köpt in nya tekniska verktyg som ska kunna upptäcka en stor del av tänkbara incidenter (IP3.24).	Av totalt 189 system så är 8 stycken i en utvecklingsfas. Mycket rör då dataminimerings-kraven. Förhoppningen är att alla ska vara färdiga till februari 2018 (IP4.24).
Vilka är de största utmaningarna gällande tillmötesgåendet av GDPR, rent processorienterat?	Awareness, att få medarbetarna mer förstående med vad GDPR innebär, vad det betyder för oss och hur vi måste arbeta i framtiden.(IP1.46)	Information, så alla anställda vet vad som gäller och lyder det som är sagt och faktiskt följer GDPR. Även inventering av system och persondata behandlingar inom Lunds Universitet.(IP2.36)	Att först definiera helt nya processer för ett företag som är så processtyrd. För att sedan få en organisation att fullt ut arbeta utifrån nya processer och rutiner. Detta förutsätter också ett stort awareness-arbete (IP3.30).	Change Management, dvs. optimering av processer så att hela organisationen hanterar alla initiativ. Gällande Data Breach, är utmaningen att svara upp till en rapportering inom 72 timmar, antingen genom manuellt arbete, eller via automatiserat systemstöd (IP4.28).
Hur ska ni göra för att tackla dessa processorienterade utmaningarna?	Utbildningar.(IP1.4 9; IP1.50)	Utbildningar med olika utbildningskanaler beroende på vem utbildningen ska nå. (IP2.38)	Tidigt anpassa verksamheten efter de nya processerna så att rutinerna och awareness-biten tidigt sitter i ryggmärgen. Dessutom måste nyckelpersoner ta på sig en ambasadörsroll som ser till att det efterlevs (IP3.36).	Att börja med att rita upp processerna och sedan efter hand inkludera alla personerna som involveras. Processbeskrivningar är en teoretisk beskrivning av verkligheten vilket gör att de kommer att testköras i case också (IP4.32).
Vilka processorienterade förändringar har ni gjort, eller planerar	För E.ON:s del handlar det om att hantera incidentrapporterin gskravet och ha rutin för det. Idag	Universitet kommer anställa ett dataskyddsombud och en person under ett år för inventering av	Förändringar av gamla processer är just nu i en identifieringsfas. Ansvaret för stora processer kommer	De processer som ligger i planeringen är bland andra den registrerades rätt att ändra, korrigera, flytta och ta bort sina

ni att göra inom den närmsta tiden?	har E.ON indicenthanteringsrutiner rent applikatoriskt men inte utifrån ett GDPR eller PUL-perspektiv.(IP1.52)	system och persondata behandlingar. Universitet har redan anställt en kommunikatör som jobbar med utbildning och information.(kolla upp mer noggrant). (IP2.42)	att ändras så att det blir en anställds enda arbetsuppgift på heltid. Denna person ska också vara en nyanställd så att de gamla processerna inte påverkar dennes arbete (IP3.38; IP3.40).	personuppgifter. Till detta hör också rapporterings-processer för respektive åtgärd. Men först måste policys för dem skrivas (IP4.41; IP4.43).
Hur förhåller ni er till att gdpr uttryckligen förespråkar privacy by design?	Det finns krav på att systemen måste kunna hantera kraven och även automatiserat till en viss del, så vi får bygga om flera system. Jag skulle säga att 80% av tiden kommer läggas ner för att lösa hur personuppgifter hanteras i systemen. (IP1.54)	Vissa system kanske har privacy by design men man har inte utvecklat det med privacy by design i tanken, utan det beror mer på vem som utvecklat systemet och deras säkerhetstänk. Vissa system kommer inte drabbas särskilt hårt för att överensstämma med privacy by design medans andra kommer.(IP2.44)	Bra, men med tanke på att det är ganska ospecificerat så hade det varit bättre att GDPR förespråkat speciella standarder istället. Samtidigt är det svårt om en lag är för detaljerad, vilket kan orsaka att lagen måste skrivas om ofta (IP3.44; IP3.46).	Det är positivt att ett regelverk slår fast en struktur för hur man integrerar person-uppgiftsbehandlingar i utvecklandet av ny systemvara eller nya processer. Det krävs antagligen en hel del tolkningar om vad exakt det innebär, men sammantaget är det positivt (IP4.45; IP4.47).
Hur ser ni på en certifiering av gdpr, både från eget håll samt mot företag ni jobbar mot?	Vi får se hur det blir med det, med vilka olika typer av certifieringar som kommer. Inga beslut huruvida E.ON kommer certifieras. Om det blir en central del på marknaden är för tidigt att säga.(IP1.56; IP1.57; IP1.58)	LDC kommer nog inte satsa på en certifiering av GDPR. Däremot kommer LDC eventuellt kräva en certifieringar från andra företag vid köp av mjukvaru och liknande. (IP2.48)	Om uppföljningen av en certifiering sker likt PCI-cerifieringar så är det bra. Det kan medföra att en granskning över potentiella partners personuppgiftshan-tering blir enklare. Detta med tanke på att det finns en skyldighet att kontrollera dem. Om de då har en certifiering från en oberoende tredje part, så underlättar det samarbetet och öppnar för en konkurrensfördel (IP3.50).	X

5 Diskussion

I detta kapitel diskuteras den insamlade empirin mot den tidigare litteraturgenomgången. Likheter och skillnader presenteras i samband med att intressanta punkter påvisas.

5.1 Förändringsarbetet mot GDPR

Moran och Brightman (2001) betonar vikten av att anta en strategi om fyra faser som strategi vid en verksamhetsförändring. Ett av momenten i denna strategi handlar om att ledaren av förändringsarbetet måste vara fullt medveten om hela innebörden av det. Till detta räknas även den omfattning om vilka organisationsdelar som berörs, samt målet med hela förändringen. I enlighet med detta, berättar IP3 att det tidigt startades ett projekt i syfte att försöka identifiera verksamhetens startposition i förhållande till de åtgärder som skulle krävas fram tills dess att GDPR börjar gälla. Moran och Brightman (2001) definierar inte vidare vad som avses med en ledarroll; huruvida det är en ensam person eller ifall det utgörs av en projektgrupp om flera personer. Däremot poängterar de vikten av att fler personer ska involveras i projektet efterhand som det drivs framåt. Enligt vår empiri är IP3 den enda av respondenterna som uttrycker sig om att dennes verksamhet har en planerad strategi i att involvera fler personer efterhand som projektet fortlöper. Detta utesluter emellertid inte att de övriga verksamheterna inte har för avsikt att involvera fler personer till projektet. IP1 säger till exempel att det övergripande projektet i Sverige leds utav två personer, men att de ständigt arbetar med informativa utbildningar genom hela organisationen - vilket är definitivt är ett sätt att integrera fler medarbetare i projektinnehållet.

Vidare skriver Moran och Brightman (2001) att en förändringsplan måste utvecklas utifrån de uppsatta målen som en verksamhet fastställer, samt att en kritisk faktor vid detta tillfälle är att inte endast utgå ifrån ett perspektiv, utan att ta in fler kompetensområden. Både IP3 och IP4 berättar att deras respektive projekt- eller programgrupp leds utav flera externa konsulter. Detta initiativ kan kopplas till den teori om att skapa fler infallsvinklar till förändringsarbetet med tanke på att konsulterna med största sannolikhet varken har tidigare eller djupare insikt i respektive verksamhet. Även IP2 nämner att LDC bland andra tagit in en jurist i arbetet med utredningarna gällande GDPR, vilket även är i enlighet med vad teorin förespråkar.
Slutligen pekar Moran och Brightman (2001), men även Patron och McCalman (2000) att informering och kommunikation är en av de viktigaste aktiviteterna vid en verksamhetsförändring. Detta dels på grund utav att mitigera de motstånd som ofta uppstår i samband med förändringar. Men även för att varje enskild individ inom en organisation aktivt ska kunna vara så pass underrättad med förändringen att de aktivt själva ska kunna bidra till förändringsarbetet, och därmed underlätta för ett effektivare projekt och realisering. IP1 berättar att just medvetenheten bland de anställda är en av de viktigaste förutsättningarna för en lyckad omstrukturering. Även IP3 talar om vikten av en bred medvetenhet inom verksamheten, samt betonar även just detta som en stor del av hela förändringsarbetet.

Sammantaget legitimeras en hel del av teorin i den insamlade empiri som vi har tagit fram genom intervjuarbetet angående förändringsarbetet. Vi anser dock att det är svårt att ställa teorin i djupare kontrast med verksamheterna eftersom dess förändringsarbete inte kommit till den fas där resultatmätningar har skett.

5.2 Tekniska utmaningar

I och med att personuppgiftslagen ersätts av GDPR kommer verksamheter behöva förändra hur man inom verksamheten behandlar personuppgifter. GDPR ställer striktare krav på bland annat inbyggnad av säkerhetskomponenter men även hur personuppgifter hanteras mellan anställda eftersom även missbruksregeln kommer ersättas.

GDPR kräver flera tekniska funktioner som påverkar hanteringen av personuppgifter inom verksamheter. Bland annat ska verksamheter kunna tillgodose information när ens personuppgifter behandlas men också ifall det sker någon typ att dataintrång eller risk som berör personuppgifterna inom verksamheten. Registrerade har även rätt att få sina personuppgifter raderade och verksamheter ska även ta bort de personuppgifter som inte längre används till det ändamål som de samlades in för. IP1 förklarar att den största tekniska utmaningen för dem är att hålla koll på dataflödet inom verksamheten, för det har dem inte krav på att ha koll på idag. Dataflödet av personuppgifter är det mest väsentliga i många av de funktioner som GDPR förespråkar. IP4 delar samma mening med problematiken med dataflödet och ser den största tekniska utmaningen som ”rätten att bli glömd” och att kunna genomföra det i samtliga, i detta fall 189 system. Därtill hör även bevisinsamling för den registrerade för att upplysa om att ens personuppgifter faktiskt har tagits bort, vilket IP3 ser som en stor teknisk utmaning men som också berör hela dataflödet inom verksamheten.

Att bygga in dataskydd direkt i systemen enligt Privacy by Design är något som GDPR reglerar uttryckligen, detta genom att använda kryptering och pseudonymisering vid hantering av personuppgifter. Freytag, J C. Kargl, F. Kung, A. (2011) menar att Privacy by Design mer är ett förhållningssätt eller ett ramverk som syftar till att informationssystem och organisationer ska sträva efter att tillhandahålla så lite information av kategorin personuppgifter som möjligt. IP2 framhäver Privacy by Design som den största tekniska utmaningen och belyser framför allt att det lätt missförstås och att resultatet grundar sig mycket på vem som tolkar det. Både IP3 och IP4 menar också att Privacy by Design framkommer som otydligt och ospecificerat, vilket de menar kommer leda till olika tolkningar om vad det exakt innebär. Cavoukian, A (2010) visar däremot hur en verksamhet kan uppnå Privacy by Design genom att fokusera på 7 grundläggande principer som syftar på att mitigera vanliga säkerhetsrisker gällande registrerades integritet.

För verksamheter betyder GDPR stora omstruktureringar på kort tid. De behöver gå igenom samtliga system och utveckla nya och uppdatera systemfunktioner för att tillmötesgå de krav som GDPR ställer. Många tekniska funktioner som GDPR förespråkar är relativt klara men

undantag finns som till exempel med Privacy by Design där samtliga intervjupersoner instämmer att lösningarna kommer vara helt olika beroende på hur verksamheten väljer att tolka det. Men även enklare funktioner kommer kräva stort omställningsarbete, i och med att samtliga intervjupersoner representerar bolag med ett flertal system, som alla måste, på ett eller annat sätt integreras för att säkra upp så att inga personuppgifter förläggs.

5.3 Processorienterade utmaningar

Hammer, M, Champy, J, & Svensson, P (1994) förklarar BPR som ett fundament nytänkande med en radikal förändring som grundar sig i att bryta ner processerna helt och börja om från början, detta för att uppnå dramatiska förändringar. Vidare beskriver Hammer, Champy, & Svensson (1994) att utvecklingen av en ny process genom reengineering som kreativitetkrävande eftersom det inte finns några tydliga tillvägagångssätt eller eventuella steg att följa. Att först definiera helt nya processer ser IP3 som en stor utmaning och syftar på verksamheten han representerar är väldigt processtyrd. Han understryker även att det är en utmaningen i sig att få organisationen att arbeta utifrån de nya processer och rutiner som verksamheten har utvecklat. IP4 belyser istället utmaningen med Change Management och menar att optimeringen av processer, så att hela organisationen hanterar alla initiativ är den största utmaningen, han beskriver deras optimeringsarbete av processer med att börja rita upp processerna för att efter hand inkludera alla personer som ska involveras.

Eftersom även missbruksregeln kommer ersättas vid införandet av GDPR, kommer det betyda att allt ostrukturerat material kommer regleras av GDPR. Det betyder att alla anställda som hanterar personuppgifter och deras arbetssätt kommer beröras. Detta påpekar samtliga intervjupersoner som ett stor utmaning med omställningsarbetet mot GDPR och benämner vikten av utbildning och information för att alla anställda ska arbeta utifrån det GDPR förespråkar. Både IP1 och IP2 arbetar aktivt med utbildningar och information och erbjuder olika typer av utbildningskanaler och inriktningar beroende på till vem utbildningen riktar sig till inom verksamheten.

Vid fall om personuppgiftsincidenter ska verksamheter enligt GDPR rapportera detta till tillsynsmyndigheten inom 72 timmar efter det att incidenten upptäckts. (Allmän dataskyddsförordning 2016/679 av den 27 april 2016). Rapporten ska innehålla specifikationer gällande incidentens art, samt på ett ungefär den mängd registrerade personer som har berörts. Rapporten ska även beskriva sannolika konsekvenser men också vilka åtgärder verksamheten har vidtagit för att förhindra eller förmildra incidentens negativa effekter (Allmän dataskyddsförordning 2016/679 av den 27 april 2016). IP4 ser ett stort processorienterat problem med både de tekniska verktyg som behövs för att identifiera incidenter men även hur verksamheten ska hantera dessa incidenter och kunna svara på de 72 timmar baserat på de systemstöd de har. Än så länge har de inte tagit några beslut om hur de ska göra men han menar att det handlar om att antingen köpa in tekniska system för att undvika personuppgiftsincidenter och intrång eller gå mer in på manuella lösningar med en

grupp som vet exakt hur vi ska agera ifall en incident skulle uppstå. Till skillnad från IP4 har IP3 redan köpt in tekniska verktyg för att i ett tidigt skede redan kunna upptäcka eventuella risker, men belyser att inte fler tekniska verktyg kommer köpas in förrän man vet vilka risker som finns och poängterar att man inte vill spendera pengar i onödan.

6 Slutsats

Den forskningsfråga som denna studien ämnade att besvara var:

Vilka är de största tekniska och processorienterade utmaningarna inför förändringsarbetet mot GDPR?

I vår studie har vi strävat efter att identifiera de största utmaningarna för svenska verksamheter gällande förändringsarbetet mot GDPR. Detta har ställts emot teori som dels deklarerar olika tillvägagångssätt om processorienterad verksamhetsutveckling, men också informationssäkerhetsprinciper med hög standardnivå. Men bakgrundsstudien berör även de juridiska krav från GDPR som ställs på verksamheter vid personuppgiftsbehandling av registrerade personer inom europeiska medlemsstater.

Vår undersökning konstaterar att det finns flera tekniska och processorienterade utmaningar för verksamheter som behandlar personuppgifter inom sina respektive informationssystem. Resultatet av studien visar sig även att te sig på det sättet att de tekniska och processorienterade utmaningarna är starkt relaterade till varandra; De processorienterade utmaningarna är beroende av tekniska lösningar, likväl som de tekniska utmaningarna förutsätter tydligt definierade, och omfattande processförändringar. Exempelvis visar resultatet att tekniska funktioner behöver implementeras för att automatiskt upptäcka incidenter, och därefter behöver nya processer skapas för att hanteringen av dessa incidenter ska kunna skötas korrekt. Undersökningen legitimerar alltså en korrelation mellan de båda faktorerna där den ene aspekten av en utmaning tvingar fram en åtgärd från den andra.

De verksamheter som har undersökts i denna studie har, generellt sett, inte kommit så pass långt i sina respektive omstruktureringsarbeten att det går att exakt fastslå vilka de största upplevda utmaningarna rörande tekniska och processorienterade aspekter är. De flesta respondenter pekar istället på att själva kartläggningen av processerna och de tekniska systemen i respektive verksamhet som en av de största utmaningarna i nuläget. Emellertid befarar många av respondenterna att en stor utmaning i framtiden kommer mynna ut i att få en organisation och dess anställda att arbeta efter helt nya riktlinjer och rutiner - alltså som en funktion av tekniska och processorienterade förändringar. De menar då samtidigt att utbildning och informering kommer vara nyckeln till framgång, även om det i sig också är en utmaning - dock organisatorisk, snarare än teknisk eller processorienterad.

7 Appendix

7.1 Bilder

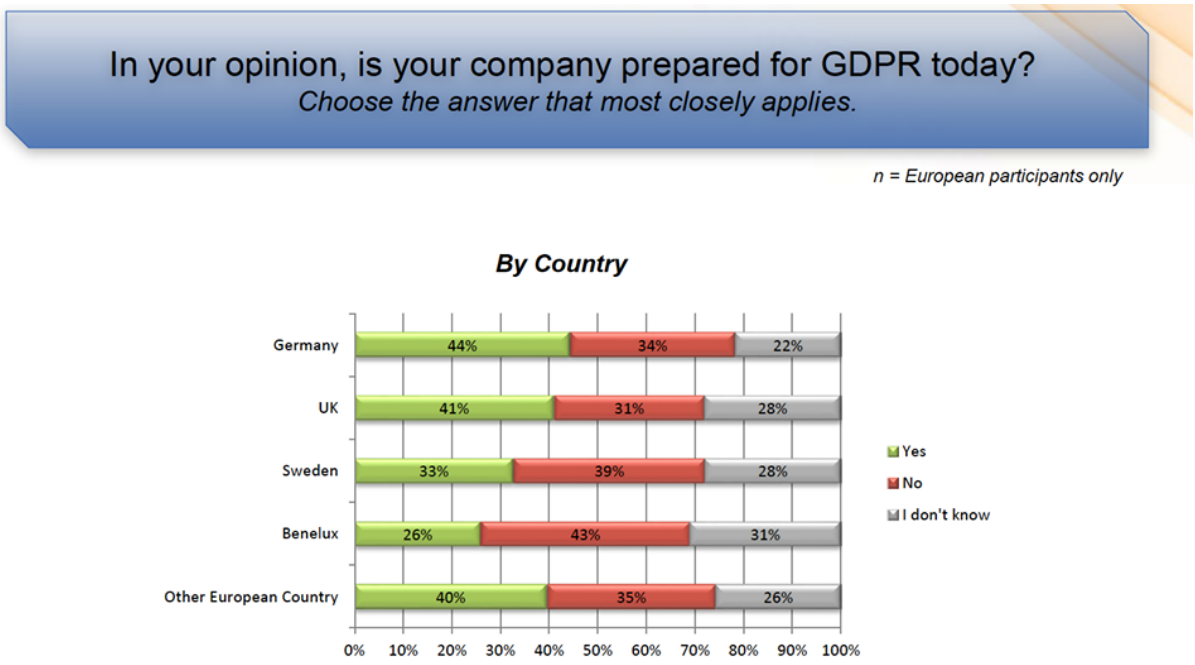

Bild 1, Undersökning utförd av Dimentional Research

7.2 Intervjufrågor

	Inledande frågor
1.	Var har du för utbildning?
2.	Vad har du för roll inom företaget?
3.	Hur jobbar ni i verksamheten för att tillmötesgå den nya dataskyddsförordningen?
4.	Hur många består gruppen av? Ingår det några externa konsulter i gruppen?
5.	Hur stor omfattning är förändringsarbetet? Hur många system berörs?
	Tekniska frågor
6.	Vilka är de största utmaningarna gällande tillmötesgåendet av GDPR, rent tekniskt, enligt dig?
7.	Hur ska ni göra för att tackla dessa tekniska utmaningar?
8.	Vilka tekniska förändringar har ni förändrat eller planerar ni att förändra för att tillmötesgå de krav som förordningen ställer?
	Processorienterade frågor
9.	Vilka är de största utmaningarna gällande tillmötesgåendet av GDPR, rent processorienterat, enligt dig?
10.	Hur ska ni göra för att tackla dessa utmaningar?
11.	Vilka processorienterade förändringar har ni eller planerar ni att förändra för att tillmötesgå de krav som förordningen ställer?
	Allmänna frågor om vad GDPR förespråkar
12.	Hur förhåller ni er till att GDPR uttryckligen förespråkar Privacy by Design?

13.	Hur ser ni på en certifiering av GDPR, både från eget håll samt mot företag ni jobbar mot?

Tabell 3:Intervjufrågor

7.3 Intervjutranskribering

7.3.1 E.ON

Verksamhet: E.ON
Intervjuperson: Ola Alsén
Yrkesroll: Personuppgiftsombud
Tid och plats: 09.00-10.00, Fredagen den 28 april 2017, möte i Malmö

Referns nr.	Person:	Frågor och svar
IP1.1	J:	Går det bra om vi spelar in intervjun?
IP1.2	O:	Ja det går bra.
IP1.3	J:	Önskar du vara anonym?
IP1.4	O:	Nej
IP1.5	J:	**Tänkte först börja fråga om din utbildning och tidigare bakgrund?**
IP1.6	O:	Jag är jurist i grunden och har jobbat med dataskyddsfrågor enda sen 2001 faktiskt, så att ja stort intresse för mig. När det gäller it-frågan, jag har jobbat mycket med it också, jobbar här på E.ON business services som är it bolaget då också plus att jag jobbar på den juridiska avdelningen med dem här bitarna. jag har liksom lite dubbelt, dubbel kompetens, vilket passar väldigt bra när det gäller de här frågorna. På den juridiska sidan har man ofta väldigt dålig it-kunskap, så den combo:n är ganska bra för att jobba med just dataskyddsfrågor, personuppgiftslagen och kommande GDPR. Så att nej, jag har jobbat med det sedan 2001, färdig jurist 1996 i Lund.
IP1.7	J:	Det är ju intressant du har juridik som bakgrund, när det handlar om GDPR liksom.
IP1.8	O:	Ja, fast många har det, fast många söker, många behöver lite extra, de vet ju inte riktigt ens vad en molntjänst är liksom. Det är lite på den nivån för de flesta jurister, så väldigt få jurister har kunskap om personuppgiftslagen och GDPR. Personuppgiftslagen och GDPR är det inte så stor skillnad på egentligen.
IP1.9	J:	Nä, det är väl lite striktare och tydligare?
IP1.10	O:	Ja, om man sammanfattar det så är det lite striktare och lite hårdare, tydligare.

IP1.11	J:	**Vilken roll inom E.ON har du just nu?**
IP1.12	O:	Personuppgiftsombud för samtliga E.ON bolag.
IP1.13	H:	Hur länge har du jobbat här på E.ON?
IP1.14	O:	Jag har jobbat lite i perioder. Men första gången 1990. Men då var det lite andra grejor, sen pluggade jag och sen så började jag faktiskt jobba här 96 och sen har jag varit lite fram och tillbaka. Nu har jag jobbat med dem här bitarna på Skanska också, mitten på 2000-talet, där jag jobbade på Skanska, var personuppgiftsombud då också för dem då.
IP1.15	J:	**Hur jobbar ni på E.ON för att tillmötesgå den nya dataskyddsförordningen?**
IP1.16	O:	Ja, vad vi kan säga först och främst har vi börjat jobba med utbildningar, för att få någon slags awareness. För att folk hör ju mycket talas om det, och det skrivs ju mycket om det men man vet ju inte riktigt vad innebär det för oss. Så vi börjar med utbildning faktiskt redan i, första utbildningen körde vi i december 2015, en breddutbildning med informationen vi hade då, så berättade vi om vad som var på gång och dem bitarna och efter det har vi kört små utbildningar då i olika konstellationer i olika små grupper. Olika bolag till exempel HR-avdelningarna, olika ledningsgrupper, på E.ON försäljningsledningsgrupp till exempel med Karins grupp då, har vi haft en genomgång och så anpassar vi dem lite utefter vilket område de jobbar med. Nu senast, denna veckan hade vi en stor utbildning, för de som var intresserade, 70-80 pers ungefär. Vi försöker få upp medvetenheten, den är ju extremt viktig, för att man bygger ju mycket system hela tiden, man bygger applikationer som är på gång och som kanske inte kommer förrän om ett år kanske två år till och med. Då måste dem ju veta så man inte bygger efter dagens modell och sen står man där, ah vi glömde det där med privacy by design, jaja just det - bygg om.
IP1.17	H:	Är det interna utbildningar då eller tar ni in experter utifrån också?
IP1.18	O:	Det låter kaxigt, men jag är så pass duktig så jag kan hålla i dem utbildningarna själv.
IP1.19	J:	Kan man säga att det är var någon top down från början, mer awareness, där 2015 och sen börjar man specialisera?
IP1.20	O:	Ja, ju mer vi vet i och med att den här lagstiftningen kommit successivt kan man säga. Först vet vi dem stora grunddragen och då börjar vi berätta om dem och sen kommer vi mer och mer in på detaljer så nu i maj kommer datainspektionen komma med mer riktlinjer och den europeiska dataskyddsstyrelsen kommer ju också successivt med lite riktlinjer. Så ju mer riktlinjer som kommer, ju mer vi får, ju mer kan vi i detalj berätta om vad som behöver göras. Därför

		har vi successivt liksom fångat in den för att sprida kunskapen.
IP1.21	J:	Jag tänkte på att du nämnde att den första utbildningen var 2015, men då hade inte GDPR kommit än?
IP1.22	O:	Då var det inte spikat än, men det var diskuterat och det fanns ju förslag och man visste, vi kände det ju då att det här förslaget kommer bli ungefär så här. Sen har man ju diskuterat politiskt fram och tillbaka, så vissa småsaker har ändrat sig sen dess då.
IP1.23	H:	Det har väl varit på gång ganska länge liksom?
IP1.24	O:	Ja, absolut det har det. Det har ju funnits utkast färdiga och det fanns det ju redan då också december 2015.
IP1.25	**J:**	**Har ni någon speciell projektgrupp, här på E.ON som ni arbetar med det här?**
IP1.26	O:	Ja det finns dels en central projektgrupp i hela E.ON som jobbar då inom Europa där alla länder är med då så vi träffas lite då och då och har lite avstämningsmöten för att kunna se om vi kan hitta synergier och likaså kunna utbyta erfarenheter, och ja fråga, hur gör ni med dem här bitarna, hur jobbar ni med dem bitarna och olika länder är olika långt framme och har olika kompetenser.
IP1.27	J:	Aha, så det är olika för olika.
IP1.28	O:	Ja precis, E.ON är ju ett globalt bolag och i varje land finns det ju jurister och it-folk som jobbar med dem här bitarna och börjar titta på det, och då har ju en grupp där vi träffas för att hitta eventuella synergier och kanske använda samma dokument för vissa delar. Sen här i Sverige har vi, man kör ju genom det lokalt, för det kommer ju vara, den svenska lagstiftningen den är, den svenska tolkningen kommer vara skillnader för vi har ju annan lagstiftning som är kopplat till det här då, tryckfrihetsförordningar och annan typ av lagstiftning och grundlagar som ibland krockar med denna lagstiftning.
IP1.29	H:	Och det är yttrandefrihet och bokföringslagen?
IP1.30	O:	Ja till exempel, så det finns ju mycket sådana aspekter man måste ta in, så därför kommer det ju vara, målsättningen har ju varit att det ska vara en gemensam lagstiftning som ska vara lika över allt, det kommer det ju inte vara riktigt.
IP1.31	J:	**Hur många består gruppen av, här i Sverige?**
IP1.32	O:	Just nu är vi bara två stycken, det är jag och en jurist till. Tanken här nu när vi ska köra projektet, för nu har vi bestämt att vi ska köra projekt för att åtgärda problem, så vi är klara fram till den 25 maj nästa år och då kommer det att vara ett övergripande projekt och där under

		kommer det ligga flera olika små projekt beroende på, för alla applikationer måste anpassas på olika sätt. En applikation kan det vara en jätteliten grej och samtidigt måste det hållas ihop för att till exempel, när vi ska göra registerutdrag så ska vi kunna hämta data som ni vet från alla olika system och då måste vi se till att det på något sätt samlas ihop centralt så man kan få upp det var och en. Varje litet projekt kan inte göra sin egen lösning där utan man måste se till att det fungerar tillsammans.
IP1.33	J:	Och att det är automatiserat och integrerat tillsammans?
IP1.34	O:	Exakt. Manuella rutiner, visst det skulle man kunna ha men det får ju inte ta för lång tid heller. Det finns krav på tidsaspekter och sen vet vi inte hur många som kommer begära de här registerutdragen.
IP1.35	J:	**Hur stor är omfattningen av förändringsarbetet för E.ON, hur många system berörs?**
IP1.36	O:	Ja du, nu tittar vi också på varje juridisk person är ju själv ansvarig för sina system, samtidigt är det många system där man är gemensamt ansvariga. Om man tittar på det totala antalet system, om varje bolag, okej ja vi ansvarar för 10 system, okej vi ansvarar för 15 men vissa av dem här hänger ihop för att det är samma system, de har sina egna personuppgifter i dem då, de är gemensamt personuppgiftsansvariga som man säger. Då har vi kanske 240-250 system, men om vi drar ner, för nu pratar vi om 10 bolag. Säg att där skulle kunna vara 40-50 system om man tänker enskilda system. Vissa är ju stora, som SAP då till exempel, är ju gigantisk stort och där är ju mycket att göra. Så då har vi gått in då och tittat då och jag har haft ett möte med varje arkitekt, det finns en arkitekt för varje applikation och systemlandskap och pratat med dem. Okej, de är juridiska kraven har vi, vi måste kunna radera på en viss tid, vi måste kunna göra registerutdrag, vi måste, alla dem här nya kraven som kommer då. Vi måste säkerställa att uppgifterna raderas automatiskt, vi kan inte ha några manuella och så vidare. Hur mycket tar det i tid för dig att fixa det här? Så har då han fått leverera, 2000 timmar till exempel behöver vi för detta till exempel, om vi tittar på SAP då som är gigantiskt. Sen kan det vara vissa som säger: “50 timmar klarar vi det på”. Utifrån det då har vi fått fram en bild, de här systemen har vi, det här behöver vi göra i respektive system, och så här mycket tid kommer det att ta och utifrån det har vi en totalbild på vad vi behöver göra. Så dit har vi kommit nu och nästa steg är att starta det här projektet, som vi tänkt starta innan sommaren. Då kommer vi från allra första början gå in i detalj, ytterligare gräva ner i varje applikation och titta på dem och se vad gör vi nu mer exakt. Sen är det ju andra aspekter också inte bara privacy by design delarna då som gör applikationen utan sen är det med policies och andra riktlinjer som ska, det organisatoriska som vi också måste fixa vid sidan om. Det skulle jag säga är den mindre biten, 80% ligger nog på privacy by design och att bygga om applikationen.

IP1.37	**J:**	**Vilka är det största utmaningarna gällande tillmötesgåendet av GDPR, rent tekniskt, enligt dig eller E.ON?**
IP1.38	O:	Det finns egentligen en sak som är den stora svårigheten och det är att säkerställa att man har koll på var alla personuppgifter finns och var de flödar och när de flyttas.
IP1.39	J:	Okej, dataflödet helt enkelt?
IP1.40	O:	Ja dataflödet, för det har vi inte krav på att koll på idag. Så i varje system vet vi att det skickas dit men sen vet man inte det här grundläggande, om var de skickar det, skickar de det till en tredje part som har cloudlösning. Så man har ju inte det här flödet idag och det har vi inte behövt ha, men nu måste vi ha det, nu måste vi veta att det skickar därifrån till dit. Sen vet vi att det skickas till den underleverantören där som har den cloudlösningen och det är den tuffa biten, att få ihop det och få koll på det och ha loggar på det som man kan logga alla flödena. Om du kommer som kund och säger, ja var är mina personuppgifter, vi ska kunna redovisa det, ja de ligger där och där och det fixar vi inte idag. Så det är absolut den största utmaningen.
IP1.41	J:	**Hur skulle ni lösa denna utmaningen?**
IP1.42	O:	Helt olika beroende på system, beroende på systemapplikationer och hur det är uppbyggt. Vi försöker ju hålla basdatan i SAP, så där ligger källdatan, vi har inte flera system så om man skickar ut uppgifter i ett system och sen behandlar lite uppgifter här ute men grunddatan /källdatan finns alltid här, här finns personer, adresser och så vidare, dem här grunduppgifterna och det kan man visst skicka till ett CRM-system till exempel och så kanske man lägger på lite, men basen, raderar man här så ska man också se till att dem här följer med. Det får inte bli massa olika egna öar där man samlar in och hämtar in lite data från olika källor, så helt plötsligt har man, där har vi den källdatan och där har vi den. Vi har ju levt i en värld här på E.ON med SAP ganska länge och nu på senare år har man ju börjat skapa massa nya system för SAP, nja lite jobbigt. Det har varit för att gränssnittet har varit lite dåligt, tagit lång tid att ändra i och sånt. Man vill ha snabba lösningar, man vill ha webblösningar, man vill ha annan typ av programvara och så kopplar man dem så man hämtar data från SAP. Därför har man ett landskap nu som är mycket större och bredare mycket mer svårövergripbart än vad man hade för några år sedan, vilket också ställer till eller gör det svårare helt enkelt.
IP1.43	J:	**Vilka tekniska förändringar har ni förändrat eller planerar ni förändra för att tillmötesgå de krav som förordningen ställer?**
IP1.44	O:	Det är ju beroende på applikation, så det kan jag inte svara på, generellt utan det är helt olika funktioner, men om man generaliserar så är det att få till en loggning som fungerar. Så man har en full check med alla uppgifter, hur de hanteras och få till loggning, få till radering

		- gallringsrutiner som också fungerar och kunna hämta ut data om du till exempel begär att få ut ett registerutdrag, ha en systematik i applikationen som gör att den kan hämta själv och sen leverera vidare till SAP som får samla ihop det och sen skicka vidare till kunden. I varje system kommer det vara helt olika lösningar, det är så splittrat landskap med olika typer av applikationer.
IP1.45	J:	**Vilka skulle du säga är de största utmaningarna gällandet av tillmötesgåendet, rent processorienterat?**
IP1.46	O:	Det är ju awareness bitarna som jag ser som viktigast, att få folk att vakna och se vad är det, vad innebär det, vad betyder det för oss, hur måste vi jobba i framtiden.
IP1.47	J:	Med policys och riktlinjer?
IP1.48	O:	Policys och riktlinjer och kunskap, kunskapen är a och o, har vi inte kunskapen ute på golvet, överallt där folk jobbar, alla jobbar med personuppgifter idag i stort sätt så kommer det fel för då bygger man applikationen utan att tänka.
IP1.49	J:	**Hur skulle ni tackla dessa utmaningar? jag gissar på utbildningar då helt enkelt?**
IP1.50	O:	Ja men det är ju.
IP1.51	H:	**Vilka processorienterade förändringar har ni eller planerar ni förändra för att tillmötesgå kraven som förordningen ställer?**
IP1.52	O:	Ja vi har inte bestämt riktigt hur setupen ska vara, nu är ju E.ON också i ett förändringsarbete just nu organisatoriskt så därför är det inte riktigt bestämt hur, var ska den här funktionaliteten, eller ja, personuppgiftsombudet som jag, den rollen jag har idag då, hur, var ska den ligga då? Ska den ligga på IT-säkerhetssidan eller ska den ligga inom juridik, eller var ska den ligga liksom. Det är mycket juridik men också lite IT och IT-säkerhetsbitar som också är involverade. Vi jobbar ju tillsammans med IT-säkerhetsavdelningen och informantionssäkerhetsavdelningen. Just nu ligger det under juridik och jag tror nog att det är där den ligger närmast men de andra måste också vara involverade på något sätt. Sen är frågan hur man ska sätta upp det, behöver man ha mer folk för att kunna managera det när det väl är igång, inte säkert, jag vet inte. Sen är det ju vissa bitar rent organisatoriskt som incidentrapporteringskravet som vi också måste hantera och som vi måste ha rutin för. Det är också en organisatorisk bit vi också måste lösa. Sen har vi ju incidenthanteringsrutiner idag utifrån applikatoriskt sätt, men inte utifrån ett PUL-perspektiv eller ett GDPR-perspektiv för det behöver vi inte ha.
IP1.53	J:	**Hur förhåller ni er till att GDPR förespråkar privacy by design?**

IP1.54	O:	Det finns ju krav på att vi måste säkerställa systemen kan hantera kraven, automatiserat till viss del. Det är ju egentligen att se till bygga om, privacy by design är ju att se till att livscykeln kan man säga, från att programmet börjar till man avslutar programmet så ska man ha tänkt på hur personuppgifterna hanteras, så det får ju inte bli ett system där man stoppar in massa uppgifter och sen ligger alla uppgifter kvar och sen dödar man system där borta och stänger man och så bara ligger det någonstans och så ligger personuppgifterna kvar. Det är typiskt så det tyvärr ibland fungerar idag. Man glömmer bort det här och så stänger man inte ner allting och så sparar man ibland undan dessutom, för att det kan vara bra att ha kvar dem här personuppgifterna vilket inte är tillåtet ens idag. Men i framtiden måste man bygga in hela det här flödet, du måste ju ha livscykeltänket på personuppgifterna i systemen inbyggt. Det är ju egentligen kontentan av privacy by design. Jag skulle säga att vi kommer lägga ner 80% av tiden för att fixa dem bitarna.
IP1.55	J:	**Hur ser ni på en certifiering av gdpr, både från eget håll samt mot företag ni jobbar mot?**
IP1.56	O:	Vi får se hur det blir med det jag har inte sett riktigt vad som kommer här med vilka typer det kommer bli tal om. Men visst det finns ju certifieringar, de pratar ju om olika symboler som kommer komma också som man kommer kunna sätta på sina sidor för att visa att man är kompatibel med det och det.
IP1.57	J:	Tror du det kommer bli en central del ute på marknaden, när man arbetar gentemot andra företag?
IP1.58	O:	Ja det är möjligt, för tidigt att säga om certifiering blir en stor del.
IP1.59	H:	Men ni siktar på att tilldelas en certifiering?
IP1.60	O:	Nej, vi har inte diskuterat om vi ska ta det. Vi får se, man kan säga att vi avvaktar lite med sådana beslut, datainspektionen har ju lovat att komma innan sommaren med alla sina riktlinjer och innan dess så tar vi egentligen inte beslut i onödan för att det kan gå stick i stäv med det som kommer nu här. Så vi får vara lite försiktiga, vi vill inte göra för mycket heller, vi vill inte lägga för mycket pengar på saker som vi inte behöver.
IP1.61	J:	Det var faktiskt alla frågor vi hade.
IP1.62	O:	Okej, ni får maila om ni kommer på något mer eller om det är något mer ni undrar över.
IP1.63	H:	Yes, vi får tacka så mycket för intervjun och att du tog dig tid.

7.3.2 LDC

Verksamhet: LDC
Intervjuperson: Magnus Persson
Yrkesroll: IT-säkerhetsarkitekt
Tid och plats:14-15, Onsdagen den 3 maj 2017, möte i Lund

Referens nr.	Person	Frågor och svar
IP2.1	J:	Är det okej för dig att vi spelar in intervjun?
IP2.2	M:	Ja
IP2.3	J:	Önskar du vara anonym?
IP2.4	M:	Nej, det går bra. Eller jag kan svara på den frågan efter jag läst igenom transkriberingen.
IP2.5	J:	**Utbildning och tidigare erfarenheter**
IP2.6	M:	Jag började läsa kemi och läste ett år kemi och sen läste jag ett år geovetenskap eftersom kemi inte var så jättekul och sen tyckte jag att jag inte riktigt hörde hemma där heller. Så var det en kompis till mig som började läsa på ADB som nu är systemvetarlinjen, så hoppade jag på det istället. Då tyckte jag helt plötsligt att jag hade hittat rätt och så tog jag en fil kand en gång i tiden.
IP2.7	J:	Arbetserfarenheter efter examen?
IP2.8	M:	Började på Tetra Pak som systemerare och programmerare och gjorde ekonomisystem. Först under 2 år, sen jobbade jag på securitas, något år som programmerare och systemerare där. Sen ville de ha tillbaka mig till Tetra Pak, så att de ringde och frågade mig om jag ville börja igen så det gjorde jag. Sen har jag dem sista 30 åren jobbat på LDC. Då började jag också med att programmera ekonomisystem och efter det var färdigt så sysslade jag med linux eller unix-rådgivning och försäljning av arbetsstationer och servrar. Sen skulle man lägga ner all försäljning, även pc-försäljning och då hade jag ingenting att göra och det var ungefär 20 år sedan och då tyckte de att it-säkerhet är något nytt så det kanske vi borde ha någon som tittar på och som börjar jobba med IT-säkerhet, så det har jag gjort senaste 20 plus åren.
IP2.9	J:	**Hur jobbar ni här på LDC angående tillmötesgåendet med den nya dataskyddsförordningen GDPR?**
IP2.10	M:	Det ligger inte på LDC:s bord att driva den frågan utan det är en fråga som universitetet centralt ska driva, vilket de gör och i slutet på förra året så började en utredning som är meningen ska vara tvådelad och den första delen är precis klar och första delen var utredning som ska beskriva hur ska vi organisatoriskt göra för att vi ska ha en chans att

		uppnå någon typ av compliance med GDPR i rätt tid. Vi kommer ju inte vara färdiga, tror vi inte, det är vi ganska säkra på, och vi kommer inte vara de enda, det är väldigt många som inte kommer vara färdiga och lite grann så gissar vi på att best effort är ganska bra, om de ser att man har en plan och jobbar på så kan inte samtliga system, samtliga organisatoriska, verksamhetsmässiga ändringar, det är alldeles för mycket. Vi måste inventera alla persondata-behandlingar vi gör och vi kommer inte vara färdiga. Vi måste rekrytera, anställa ett dataskyddsombud, vi måste säkra upp befälsgången så att säga, när det gäller it-säkerhet. För att idag så finns det ingen på Lunds Universitet, någon formell beskrivning av var informationssäkerhets ansvaret ligger, så därför är det lite delat mellan olika människor, vissa har haft delar av ohejdad vana och andra har sett att här har varit ett litet vakuum och så har de tagit ansvaret så att vissa delar överlappar och vissa delar kanske faller genom stolarna, men det övergripande ansvaret har aldrig delats ut när det gäller informationssäkerhet. IT-säkerhet är en sak, där är vi ganska klara över hur det funkar men informationssäkerhet, det vill säga det greppet som både innehåller IT och information, hela den biten är inte riktigt 100% klar exakt var allt ansvar ligger, så det är en annan sak som måste fastställas av förvaltningen. För förvaltningschefen måste berätta att, det här ska göras och det ligger på den här funktionen, så det är en annan sak som ingår i det arbetet.
IP2.11	J:	Angående att ni inte anser att ni kommer hinna vara färdiga, beror det på att ni upplever att det är för kort tid från det att lagen presenterades till att den ska initierats och verkställas, så att säga?
IP2.12	M:	Ja asså, universitet av den här storleken har ju en ganska lång startsträcka. Det är fruktansvärt decentraliserat. Var och en fakultet, var och en institution står på egenbestämmande rätt och vi har haft tidigare PUL-ansvariga som har jobbat med det här 20% och inte haft en möjlighet att följa upp vilka personuppgiftsbehandlingar har vi, är alla rapporterade, utan det har varit väldigt mycket. En del är duktiga och rapporterar vad dem behandlar för någonting och andra vet inte ens om det, vissa människor vet inte ens vad en personuppgift är och kanske behandlar personuppgifter och inte tror att det är personuppgifter och andra tycker att det här är ostrukturerat och så litet så att, amen. Så att det är väldigt stor utbildningsinsats som kommer behövas också. Så att de permanenta förändring som den här utredningen, första delen föreslår, inrätta en funktion som dataskyddsombud på heltid, så att 20% räcker inte, det här måste vara en heltidstjänst. För att det är inte bara att rapportera in och föra ett register utan det här måste följas upp med utbildning och allt. Dessutom så, GDPR ger ju dataskyddsombudet mycket större krav, mycket större rättigheter och de ska rapportera direkt till ledningen och lite sådana här saker. Så att, dataskyddsombudet kommer ha en mycket större juridisk makt. Läser ur utredningen: Peka ut ett tydligt ansvar för informationssäkerhet på gemensam nivå. Se till att arbetet med relaterade områden samordnas inom förvaltningen. För att personuppgifter har vi på väldigt många olika ställen, fruktansvärt

		många ställen och det är allt ifrån excelark till ladok och stora system, det finns över allt och forskningsdata har lite särställning inom personuppgifter och det finns ju flera olika orsaker varför man får lov, man kan ha tillstånd som myndighet för att bedriva myndighetsutövning. Då har man ett automatiskt tillstånd och då behöver vi inte be om lov och då får vi föra personregister och sen så kan du ju be respektive person om lov och få behandla för vissa ändamål och sen så kan du via avtal. Jag är anställd, jag har ett anställningsavtal då ger jag också rätt att de ska sköta min lön, det vill säga ha ett lönesystem, då behöver de inte fråga mig om lov för att då har vi ett avtal. Sen är det forskningsändamål, där behöver man inte heller be om lov, du kan behöva be om lov. Sen exakt hur det kommer att ske är vi lite osäkra på, eftersom det är tre stycken utredningar på gång. Det är tre statliga utredningar på gång som rör GDPR, den första är klar nu i maj och de är GDPR inom statsförvaltning. En är klar efter sommaren, början på hösten och det är GDPR för utbildning och den sista för GDPR är för forskningsdata och kommer i december. Innan de kommer är vi inte riktigt säkra på exakt hur lagen kommer att gälla för våra olika delar, för alla de här tre kommer gälla för oss.
IP2.13	J:	Den här utredningen den var gjord utav?
IP2.14	M:	Den här gjord av Kristina Arnrup Thorsbro och Pernilla Skantze, Kristina jobbar i förvaltningen, just med utredningar. Pernilla som är jurist och jag, och det är vi tre som har skrivit den här.
IP2.15	J:	Själva arbetet är det någonting som kommer falla på LDC sen?
IP2.16	M:	Nej, det här lämnas till förvaltningschefen, ett universitet är uppdelat i två bitar, det som är forskning och utbildning, där är rektorn chef och det som är förvaltningen och det är liksom alla stödsystem runt omkring, ekonomi och löner och allt sånt där och där är förvaltningschefen chef och rektorn är chef över allihop, även förvaltningschefen. Men förvaltningschefen har då uppdrag som sköter all förvaltning och det är förvaltningschefen som kommer att ta beslut rörande de har grejerna, vad som måste göras.
IP2.17	J:	Men vem är det sen som kommer utföra det i så fall?
IP2.18	M:	Då får man lämna ett beslutsunderlag till förvaltningschefen som är överenskommet så att hon är nöjd med det och då kan hon ta ett beslut om till exempel, där kommer många olika beslut, ett beslut för att inrätta ett dataskyddsombud och vilka uppgifter dataskyddsombudet ska ha och så vidare. Ett beslut för att peka ut ansvariga för it-säkerhet och då ska det också stå vad som ingår i IT-säkerhet, vad är uppgifterna för en it-säkerhetsansvarig, då tas det ett beslut. Men sen är det sådana här saker som att, se till att relaterade områden samordnas inom förvaltningen och det är till exempel, för tillfället så är det väldigt mycket prat om forskningsdata, därför så är det åtminstone tre olika utredningar på olika

		ställen, LUNARK som är superdatacentret, är ansvariga för en utredning. Kansli HT, kansli SV, samhällsvetenskap de har gjort en utredning och UB håller på med en utredning. Just om forskningsdata och hur man ska hantera forskningsdata, mycket med open data och sådana här saker och hur vi ska inventera så att om vi har forskningsdata så ska vi kunna återanvända den. Vad har vi för register, vad vet vi? Vad har vi för forskningsdata? Hur skapas den? Hur behandlas den? Hur lagrar vi den? Hur arkiverar vi den och vilken forskningsdata får vi ha? Vad är känslig data? Vad kan vi sprida? Det är massor av frågor där. Det är så nära GDPR och persondata så det hade varit väldigt bra om man hade kunnat samordna de här inventeringarna och kanske samla dem i samma eller liknande register. Sen är det att bygga upp strukturer och rutiner för stöd och och hjälp till hela universitetet.
IP2.19	J:	Till exempel den punkten när alla utredningar är färdiga och man har fått en uppfattning om vad som behövs göras med olika system kanske till och med vissa system behöver ändras och så vidare, vem är det i så fall som omstrukturera dessa systemen och bygga om dem?
IP2.20	M:	Orsaken till att vi gjorde den här i två delar det är för att efter del ett kan vi börja jobba och sen så kommer den andra delen av utredningen att löpa parallellt men den kommer vara ganska mycket, vad ska vi göra? I och med denna så kan vi alltså få personal på plats som sen under nästa utredningsfas vet vad de kan börja jobba med. Bland annat så är det, vad ska ändras och nästa fas kommer att beskriva det. Vad måste våra system uppnå för någonting, vi måste kunna exportera data så du som privatperson kan komma att säga; jag vill inte vara med i ert system, jag vill vara med i något annat så ni måste exportera min data. Jag har rätt att bli glömd, vi måste kunna radera data från en privatperson. Det här kan tas tillbaka till samtycke för fortsatt så att, ja vi kan behålla data men vi kan inte ta in mer data av den här personen. Massa sådana saker som systemet idag kanske inte kan göra allt det här och då kan vi inte upprätthålla den här lagen och då måste vi göra förändringar i system. Alltså måste vi ha en lista över saker och ting som behöver våra system måste klara och så lämnas den till systemförvaltarna. Varje större system vi har, har en systemförvaltare, någon som äger systemet och de har också de ekonomiska ansvaret och då får de listan och då kommer de gå till den som utvecklar systemet. Det kan vara här på LDC, det kan vara ekonomisystemet som driftas av CGI och det heter Raindance och det är köpt av en firma och det är inte vi som driftar det, servrarna står i källaren men det är inte vi som driftar det, så då får de gå till CGI och fråga, uppfyller det här systemet dem här kriterierna? Om dem inte gör det så får de ett stort problem, för då måste dem gå till utvecklarna Raindance och begära en ändring och det går ju inte speciellt snabbt. Det är ett jättesystem och det får ju läggas i deras utvecklingscirkel och de har några releaser några månader fram eller år fram och våra system här som vi själva utvecklar, samma sak där. Då får systemägaren som för det mesta sitter på förvaltningen till exempel personalsystem så är det personalavdelningen som har en person, ekonomisystem så är det en

		ekonomiavdelningen som har en person som är systemförvaltare, är det Ladok eller utbildningsgrejor så är det student och utbildning som är den organisationen på förvaltningen som äger systemet och då får de titta efter, vi måste fixa det här och sen så har man möte tillsammans med de som driftar systemet och dem som utvecklar systemet, klarar vi det här? Och så får man bocka av och sen så om man inte gör det får man göra en plan över hur vi ska göra. Det är sånt här som privacy by design, har vi för mycket data i systemet? Har vi data vi inte behöver? Har vi persondata vi inte behöver så får vi radera den, vi får inte ha den längre. Så att det kommer vara en väldig massa punkter som ska ställas samman och det är nästa del av här arbetet. Stora centrala system har vi inga problem med, dem känner vi allihopa. Hela förvaltnings systempark åtminstone ner till en viss minsta nivå sköts enligt en systemförvaltarmodell som heter PM3 och den är inköpt och lite tweakad så den passar oss och där står precis vem som äger systemet, vem som ska drifta och hur ska man bestämma om förändringar i systemet och allt sånt där. Modell för hur man förvaltar ett system och där är väldigt enkelt, där vet vi alla och där är bara att skicka information och de är ju vana vid modeller, de är vana att behandla system och underhålla system.
IP2.21	J:	**Hur många består projektgruppen av?**
IP2.22	M:	LDC har ju suttit och väntat ut denna utredningen så det har inte funnits någon orsak för oss att göra något direkt på egen hand innan den här är klar. Sen kommer vi att följa det arbete som görs centralt och följa med där. Min roll som informationssäkerhetsansvarig på LDC är att se till att alla vet om att det här kommer, så det inte blir någon överraskning. Sen får vi vänta, dels får vi vänta på när dem centrala kraven kommer när våra systemägare kommer få information från centralt håll att nu måste ni titta igenom dem här sakerna, det här är saker som ni måste se till att era system klarar av att göra. Då kommer de komma till oss och då kommer vi få sitta ner och försöka bocka av vad som är okej och det vi inte klarar av. Sen får man göra en plan, när kan vi göra förändringar så att vi klarar GDPR och sen får de avsätta tid och pengar. Så länge man jobbar på det så känns det ju som att även om man skulle gå över gränsen i maj nästa år så bara man har den här planen så känns det inte som man skulle drabbas av några böter i alla fall. För att alla kommer inte vara klara, även hur mycket man än jobbar så kommer inte allt till hundra procent vara klart. Men vi har börjat tidigt, relativt tidigt i alla fall tycker jag och här finns en plan och här finns en strategi och sen vi som liksom i andra hand som LDC är ju en sådan här andrahands ansvarig. Så vi har ju i princip inget eget ansvar utan vi väntar på att någon berättar vad dem behöver och sen försöker vi göra de delar. Medan förvaltningen som äger systemen måste sätta sig ner ganska snabbt och börja fundera på vad som måste göras. Sen kommer dem till oss eller så kommer de till de andra små systemen, och sen kan vi börja arbeta och sen kan ekonomisystemansvariga prata med de som äger

		Raindance för ekonomisystem. Vad gäller Ladok så är det Ladokkonsortiet som äger Ladok och det är alla förändringar där måste göras av Ladokkonsortiet som sitter i Umeå. Personalsystem som heter Primula är ju utvecklare som inte finns här heller utan då måste dem gå till de som programmerar Primula. Men alla de system som äger och driftar och har gjort här, får ju vi göra förändringar i.
IP2.23	J:	**I en sådan förändring, hur stor skulle en sådan grupp bestå av då?**
IP2.24	M:	Det är ju alldeles upp till vad det är för system. Förändringar i Ladok, det är ett statsregister och det finns inte så många statsregister, det är alltså Ladok för studerande, kriminalvården, sparregistret och så är det skattemyndighetens register. Så det är några stycken som regeringen är beslutare att de måste finnas och det är definitivt en myndighetsutövning så där kommer du inte ha rätt att bli glömd, vi behöver inte begära något tillstånd, vi behöver inte meddela personer att de finns i registret och så vidare. Där kanske kommer behövas några förändringar, kanske så att vi sparat för mycket information så att privacy by design inte är uppfyllt. Men det blir ju en sak som Ladokkonsortiet tittar på. De sitter ju i Umeå så det är inte vi som behöver driva den pucken.
IP2.25	**J:**	**Hur stor skulle du säga förändringsarbetet är? Hur många system berörs totalt?**
IP2.26	M:	För LDC:s del, för vår interna del så tror jag inte att det är många, för LDC som sådan, en handfull kanske fem system kanske, jag gissar helt vilt. Vi har inte jättemycket persondata i system. Vi driftar maskiner, vi driftar servrar, vi driftar system, det känns inte som det är så väldigt mycket persondata. Vi har intern webb, vi har egen ekonomihantering och lite sådana här saker och dem kommer innehålla persondata men inte så jättemånga system. Men system som vi har utvecklat till andra som vi inte själva kör för vår egen personal utan vi kör för andra, de är säkert några tiotal, kan jag tänka mig.
IP2.27	J:	**Vilka skulle du säga skulle bli de största utmaningarna gällande GDPR rent tekniskt?**
IP2.28	M:	Det är lite knepigt att säga, men jag kan ju tänka mig att det här som heter privacy by design, systemen ska vara gjort så att personlig integritet är skyddat och inbakat i systemet. Det ska vara skyddat utan att du ska göra ytterligare saker. Systemet ska vara designat så att din personliga integritet är skyddad och är det inte det så kan det nog vara svårt att in det så att säga. Är det för öppet i sig så kräver det kanske en hel omstrukturering av hela systemet. Om vi ska säga de här bitarna, rätten att bli glömd kan ju vara nog så svår, att ta bort alla spår av en person ur ett system. Men sedan sådana saker som rätten att bli glömd, kunna exportera all data om en person, det är ganska enkla saker för dem är lätta att förstå, det går inte att missförstås. Privacy by design kan missförstås, vad är privacy by design? Ingen aning, det är upp till vem

		som tittar på det. En del kan ju säga att det här är privacy by design men vilken verkshöjd ska den ha då?
IP2.29	J:	**Hur skulle du i så fall säga att man skulle göra för att tackla dess utmaningarna rent tekniskt?**
IP2.30	M:	Ingenting är ju egentligen ett tekniskt problem. Det är tid och det är pengar och resurser, allt består av de tre sakerna och minskar du den ena för du öka den andra. Det löser alla problem, har du tid och har du pengar och resurser så löser du alla problem och problemet är att vi inte har resurser, då kan vi ösa på mer tid och mer pengar, eller har du inte tid så får vi ösa på mer resurser. Vi kommer inte att kanske tillsätta så mycket pengar för vi har en begränsad budget, man kommer nog inte få så mycket extra för det här. Tiden är väldigt begränsad, vi vet exakt när det ska vara klart och LDC kan inte tillsätta mer resurser än vad vi har folk. För det mesta arbetar alla redan hundra procent, vi sitter inte här och såsar och dricker kaffe för det mesta.
IP2.31	J:	Finns det någon idé då att ta in extern hjälp?
IP2.32	M:	Kanske, det gör vi av och till, man vet aldrig. Har man inte tid att göra det själv, ibland behöver vi kompetens och ibland behöver vi bara folk för att vi inte har tillräckligt med personal. Så att det är inte alls omöjligt.
IP2.33	J:	**Vilka tekniska förändringar har ni eller planerar ni att förändra för att tillmötesgå de krav GDPR ställer?**
IP2.34	M:	Nej, inga tekniska förändringar än. Där är ingenting gjort.
IP2.35	**J:**	**Vilka är det största utmaningarna rent processorienterat?**
IP2.36	M:	Den största utmaningen kommer att vara information, informationskampanjen där alla människor vet vad som gäller och att dem faktiskt sen lyder det som är sagt, att de faktiskt rapporterar in sina system och att de vet vad som gäller och faktiskt följer GDPR. Så utbildningskampanjen kommer vara stor, den kommer bli ganska massiv, det tror jag kommer vara ett av de största och den näst största kommer vara inventering av system för vi har så fruktansvärt många system och det är så många ställen de ligger på och varje gång dem går ut måste man berätta för alla där, det här är vad vi är ute efter, GDPR betyder detta, persondata är det här och att göra det för två hundra ställen och försöka få alla att fatta. För att det kan finnas överallt bland personalen, du kan gå till prefekten eller sekreteraren och fråga och de har ingen aning. De har ingen överblick idag över samtliga system som finns hos samtliga personer. Så att det kommer vara ett jätteproblem, att vi får med oss allt eller åtminstone så mycket så att vi har en vettig bild över vilka personregister som vi har.
IP2.37	J:	**Hur ska man tackla dessa utmaningar? Du sa utbildningar?**

IP2.38	M:	Utbildning kommer och det har vi en kommunikatör som jobbar halvtid och ska se till det, och där kommer behövas mycket mer personal under vissa tidpunkter när det här ska realiseras och det kommer behövas kanske webbutbildning, det kommer behövas webbsidor och det kommer behövas massa olika utbildningskanaler beroende på vem du ska nå. Alla ska ha någon typ och det är ganska basic som förhoppningsvis kan få alla att läsa men vissa kommer behöva en ganska detaljerad utbildning och då ska det finnas utbildningsalternativ för alla som är riktade, så det kommer ta sin lilla tid.
IP2.39	J:	Och när det gäller den näst största utmaningen, som var med inventeringar och så, hur ser du att man skulle gå tillväga där?
IP2.40	M:	Här kommer det att anställas en person för inventering, inventeringen kommer antagligen att skötas av UB så biblioteken kommer att få en ganska stor roll i det här. Biblioteken är väldigt duktiga med det här med data och kategorisering, det är vad dem håller på med, det är deras jobb. Man försöker ta expertis därifrån och hjälp därifrån. Så vad jag vet så kommer dem att vara drivande i inventeringen.
IP2.41	J:	**Vilka processorienterade förändringar har ni gjort eller planerar ni att förändra för att tillmötesgå GDPR?**
IP2.42	M:	LDC kommer nog göra mer än kanske behöva en konsulttjänst eller två, så vi kanske behöver ta in lite konsulttimmar. Universitetet som helhet kommer anställa ett dataskyddsombud. Vi har under ett år i alla fall en kommunikatör som kommer jobba med utbildning och kommunikation. Under ett år en person för just inventering och den personen kanske blir samma som dataskyddssombudet, det vet vi inte. Vi vet inte om dataskyddsombudet kommer att vara en delad tjänst eller kommer vara en tjänst plus en halv till. Vi vet inte var den kommer att ligga, om den ligger på det juridiska eller inte, det är för tidigt att säga. Sen också de förändringar som kommer ske på universitetsbiblioteken om det nu så att utbildning som satsas kommer kanaliseras via biblioteken eller om biblioteken kommer att vara dit forskarna ska vända sig för att få reda på vad som gäller. Så där kommer bli lite förändringar.
IP2.43	J:	**Hur förhåller ni er till att gdpr uttryckligen förespråkar privacy by design?**
IP2.44	M:	Vissa system kanske har det men jag tror inte att tanken har varit privacy by design. En del är väl mer, en del programmerare och systemerare är väl mer paranoida än andra och tycker att nä, vi behöver inte det här, då ska vi inte ha det heller. Men just tanken privacy by design tror jag inte utan programmerare är oftare mer av principen av att det kan vara bra att ha. Passport där man går in och byter lösenord till exempel är ganska paranoid kille som gjort och där tror jag inte uppfyller privacy by design till exempel. Lite på grund av att vi vet att det är ett väldigt känsligt system, du kan inte tillåta att fel person byter

		lösenord åt någon annan. Så där är säkerheten lite högre, eller ganska betydligt högre än av många av de andra systemen. Där är det nog inte heller så att där dräller massa personuppgifter heller mer än nödvändigt. Vissa kommer säkert flyga ganska lugnt och inte behöva något annat medans några andra kommer inte flyga alls, där inte tanken ens har varit att, jag vet ett till exempel där jag vet att dem lagrade en massa känslig uppgifter som definitivt inte kan räknas som privacy by design för att systemet inte är gjort på det sättet och jag vet att det lagrar känslig information.
IP2.45	J:	**Hur ser ni på en certifiering av gdpr, både från eget håll samt mot företag ni jobbar mot?**
IP2.46	M:	Så som jag har läst lagen finns där ingen möjlighet att certifiera och det finns inga krav på certifiering. Att sen massa konsultfirmor går ut och säger i princip att jo vi kan certifiera för GDPR.
IP2.47	H:	Det står i förordningen att det finns möjlighet att certifiera
IP2.48	M:	Av datainspektionen? Det tror jag inte dem har tid med. Vi kommer nog inte satsa på att certifiera oss men vi kanske kommer kräva det. En annan stor del av jobbet mot GDPR är att se till att vår upphandlingsenhet, när man upphandlar saker, att de verkligen vet och vad de ska kräva, vad kräver GDPR och att vi inte köper molntjänster eller system som inte uppfyller de här kraven. Så det är en annan grupp som måste ha ganska god kunskap i vad som gäller.
IP2.49	J:	Det var alla frågor vi hade faktiskt. Är det något du vill tillägga?
IP2.50	M:	Nej
IP2.51	J:	Då får vi tacka så mycket.

7.3.3 Företag X

Bransch: Bank.
Intervjuperson: Michael Lindström.
Yrkesroll: Chief Information Security Officer.
Tid och plats: 15.00-16.00, Måndagen den 8 maj 2017, möte i Helsingborg.

Referens nr	Person	Fråga eller svar
IP3.1	J:	Godkänner du att vi spelar in intervjun?
IP3.2	M:	Ja.
IP3.3	J:	Du har rätt att vara anonym om så önskas, så är detta något du vill vara?
IP3.4	M:	Det beror ju på frågeställningen, så det kan vi se senare. Men preliminärt, nej, jag behöver inte vara anonym.
IP3.5	H:	**Då börjar vi med lite allmänna frågor om dig, samt om företaget. Vilka studiebakgrunder, samt tidigare erfarenheter har du sedan tidigare?**
IP3.6	M:	Jag kommer ju från industrin, så det finns ju ingen utbildning som har med mitt specifika arbete att göra. Utan det mesta utav de roller jag jobbat med tidigare har krävt ständiga uppdateringar, samt en hel del timmar varje månad kring leverantörsspecifika saker, eller dokument att läsa igenom för att kunna lösa nästa veckas arbetsuppgifter. Mycket har då med problemlösning att göra om man ser tillbaka på det rent tekniskt. När man arbetar med IT som konsult, så skulle jag vilja påstå att det handlar mycket om ständigt lärande varje dag. Sedan har jag gått en hel del leverantörsspecifika utbildningar och certifieringar genom åren; allt från Microsoft, HP, Cisco, Blue Coat och 3COM. På senare tid, det vill säga de sista 15 åren, så har det handlat med om att få en stämpel på att man faktiskt kan det som man lärt sig genom åren. Och då har jag ju fått CISSP-, och CISM-certifieringar från de stora internationella säkerhetsorganisationerna ISACA och isc2.
IP3.7	J:	Snabb följdfråga; Vad står CISSP och CISM för?
IP3.8	M:	CISSP står för “Certified Information Systems Security Professional”, och CISM står för “Certified Information Security Manager”.
IP3.9	J:	Okej, fortsätt gärna.
IP3.10	M:	Så de tillsammans berör ju de olika områdena och inriktningarna som finns, även om båda två berör säkerhet. CISSP är väldigt omfattande och berör egentligen det mesta inom IT, medan CISM handlar mer om kontroll och regelverk ur ett management-perspektiv. Med andra ord har jag ingen universitetsutbilning, vilket jag i och för sig inte anser vara någonting negativt, utan jag tror att många IT-utbildningar har en tendens

		att vara lite utdaterade. Förvisso finns det en hel del moment som inte ändras genom åren, till exempel hur man gör vissa uträkningar, eller specifika metoder och så vidare. Men ibland har jag en känsla av att lärarna eventuellt gör det för bekvämt för sig själva, och inte uppdaterar utbildningarna enligt hur det ser ut ute i arbetslivet. Och när det gäller IT så händer det så fruktansvärt mycket; det som är dagens fakta, gäller kanske bara sex månader framöver innan det kommer nytt. Detta är ju samtidigt något som har gått fortare och fortare de senaste 15 åren. Därför tycker jag det är viktigt, och bra att läroverken plockar in föreläsare från arbetslivet som får ge nya aspekter och nya infallsvinklar till studenterna - det är en jätteviktig input helt enkelt. Detta, så att man inte står där som nyexaminerad och blir chockad för att ingenting stämmer överens med vad man precis lärt sig från skolan.
IP3.11	J:	**Okej. Vad är din roll på Företag X?**
IP3.12	M:	Den engelska titeln är CISO - alltså Chief Information Security Officer. med andra ord "Informationsäkerhetschef" på svenska, ungefär.
IP3.13	J:	**Hur jobbar Företag X med att tillmötesgå den nya dataskyddsförordningen, GDPR?**
IP3.14	M:	Företag X har, sedan rätt så många månader tillbaka, startat ett projekt som numera består utav flera stycken mindre projekt - vi har alltså breddat scop:et. Första delen av projektet handlade mycket om att förstå var Företag X stod någonstans. Parallellt med detta så bestämde vi oss för att splitta upp det vi hade förstått. GDPR innebär ju awareness, titta över policys, regelverk, rutiner, ramverk och organisation. Så efterhand som vi har fått mer information, så anser jag att projektet numera är redo för att ta beslut för andra åtgärder som man till en början kanske inte hade klart för sig. Så med andra ord har vi avsatt väldigt mycket tid och resurser för GDPR, redan sedan förra året egentligen.
IP3.15	J:	**Hur många personer består projekt-gruppen av, och finns det några externa konsulter involverade?**
IP3.16	M:	Ja, till att börja med så är ju bland annat projektledarna externa konsulter. För några veckor sedan så tror jag att vi kom fram till att vi var cirka 15 stycken som aktivt arbetar med GDPR. Men ju längre tiden går, så blir det fler och fler i verksamheten som involveras mer och mer. Detta för att det helt enkelt blir mer att göra efterhand som tiden går. Så efterhand som varje system är färdiggranskat så ska åtgärder tas, och då blir det därmed fler och fler mini-projekt. Antingen är det då systemägarna eller processägarna för respektive åtgärdsdel som tar över dessa mini-projekt och sedan utför detta enligt anvisningar - och på så sätt sväller ju också omfattningen av projektet. Så vi är ju på toppen av isberget av själva projektet, så att säga.
IP3.17	H:	Hur långt har ni kommit i förändringsarbetet?

IP3.18	M:	Ja, vi har ju arbetat i olika steg. Jag tror att organisationen i princip redan är satt - alltså hur den ska se ut från och med att GDPR börjar gälla. Det är förvisso en mindre bit. Sedan är ju Legal-avdelningen färdiga med att titta över och kartlägga vilka dokument som GDPR påverkar. Så just nu håller de på att skriva om dessa dokumenten, och de är kanske färdiga någon gång innan sommaren. Awareness-delen är ju däremot en stor bit, och utbildningar har ju skett fortlöpnade i projektet med deltagare av berörda delar. Jag håller på med själva utblidningen som ska vara fortlöpande - alltså awareness-utbildningen för GDPR - och detta kommer också vara färdigt och ligga i vår digitala inlärningssystem lite innan sommaren. Så sakerna är gjorda, men det är ju en levande process med tanke på att det ska gås igenom med alla delar och alla ska vara införstådda och ta allting till sig. Kartläggningen är i princip gjord, det vill säga att vi har hittat alla system som berörs. Själva arbetet med varje system i sin tur är nu i full gång. Där återstår kanske 65-70% arbete med att dokumentera ner om vad som ska göras - en del system beslutas om att läggas ner helt och tas bort, andra system måste åtgärdas, och vissa system ska bytas ut hel mot ett nytt. Så det är i denna beslutsfattande fas som vi är i just nu.
IP3.19	J:	**Okej. Hur många system berörs totalt av någon form av åtgärd?**
IP3.20	M:	Nja, det vet jag faktiskt inte exakt. Jag vet bara att alla system är identifierade, sedan exakt hur många det är kan jag inte utantill. Däremot tror jag att merparten av alla system berörs på något sätt, tyvärr.
IP3.21	J:	**Okej vi förstår. Vi går över till frågor rörande tekniska utmaningar; Vilka är de största utmaningarna gällande tillmötesgåendet av GDPR, rent tekniskt, enligt dig?**
IP3.22	M:	Det är i så fall, om man tolkar det rätt, nivån på straffavgiften - administrativa avgiften - och tidsaspekten på att svara upp på en incident. Då tror jag att det viktigaste är att investera i verktyg som kan automatisera upptäckt, samt bevisinsamling för att kunna rapportera. Och jag tror att om man tar bort andra tekniska saker som man tror sig behöva, så är detta det viktigaste.
IP3.23	J:	**Okej. Vad anser du då att vara det rätta sättet att tackla denna tekniska utmaningen?**
IP3.24	M:	Ja, utan att gå för mycket in på detalj, så håller vi just nu på att skriva om hela vår incidenthanteringsprocess, just med tanke på att det råder ett annat tidskrav än tidigare. Vi har dessutom köpt in verktyg för detta - lite tidigare än väntat. Dock inte alla verktyg som behövs, men just de som behövs för att kunna upptäcka en stor del av incidenter; de är redan inköpt. Sedan återstår ju att implementera dem och så vidare, givetvis. Men det är först efter man gjort sin kartläggning, och förstått hur man får in samt hanterar sin information som man inser vilka risker som finns. Och först då kan man ta ett beslut om vilken, och hur mycket teknik som

		måste köpas in för att klara av tidskraven. Viktigt att tänka på i vår situation är ju att vi inte bara köper in den dyraste och bästa tekniken, för att sedan upptäcka att den nödvändigtvis inte behövdes. Så i detta skedet handlar det mycket om risktänk, och vi måste hela tiden ställa oss frågan om vi faktiskt behöver köpa in ny teknik eller inte. Sedan dessutom; är det rätt läge just nu att köpa in det, eller bör vi vänta? För man vill helt enkelt spendera för mycket resurser på fel saker och i fel tillfälle på grund av att det kanske finns viktigare saker på agendan. Helt plötsligt så kanske det resulterar i att vi prioriterar fel saker och därmed tappar tempo. Det stora arbetet är helt enkelt kartläggningen, och gå igenom alla systemen - det är det som tar mest tid just nu.
IP3.25	J:	**Okej, Du har delvis varit inne på det i förra svaret, men nästa fråga är: Vilka tekniska förändringar har ni genomfört, eller planerar ni att genomföra just nu?**
IP3.26	M:	Ja, precis. Men det handlar om att få bättre kvalité i själva incident-upptäckningen. Idag är det lite för mycket reaktivt - det är inte förrän flera saker händer samtidigt som någon eller något system reagerar, och sedan börjar arbeta med problemet. Så, det som kommer att bli den stora skillnaden är att; de som jobbar med incidenter kommer att se det innan någon annan märker det - tanken är ju att hinna sätta igång åtgärder samt till och med begränsa skadan innan något överhuvudtaget kommer fram. Det är ju hela vinsten med det hela, plus att vi får så mycket information att vi kommer att kunna ta bättre beslut om hur stor insats vi behöver göra. Jag tror att de flesta företag idag inte har den kollen. Det är i alla fall min erfarenhet från min tid som konsult - företag har helt enkelt inte den kollen på sin verksamhet. GDPR kommer att tvinga fram att man får betydligt större kontroll än vad man någonsin tidigare haft.
IP3.27	H:	**Okej, ja. Har ni gjort några förändringar i systemen eller liknande inför GDPR?**
IP3.28	M:	Ja, om jag tolkar det rätt så ja. Men nu sitter jag ju med som en referens i gruppen. Det vill säga att vi har synpunkter på vad som görs och inte görs, dock inte hur det görs. Men det jag hör där är ju att när man väl går igenom systemen, så ifrågasätter man ju varför information finns på specifika ställen och hur mycket handlar om, samt vad man kan göra i övrigt. I varje utvärdering av varje system, så har vi ju till exempel lagt till saker som handlar om allmän kontroll, best practice och lite sånt. Så att hela dokumentationen av systemen kommer ju att få ett upplyft, och det behöver inte vara saker som har direkt med GDPR att göra, utan rent allmänt för att förbättra systemen - en allmän uppdatering av dokumentationen helt enkelt.
IP3.29	J:	**Då går vi över till det processorienterade perspektivet; Vad anser du är de största utmaningarna rent processorienterat, gällande tillmötesgåendet mot GDPR?**

IP3.30	M:	Ja, organisation är inte så svårt att sätta, och att rita upp en process inte heller svårt. Men däremot att få en organisation att jobba enligt processen är själva utmaningen. Många jobbar ju enligt vissa rutiner idag, som inte stämmer längre. Och nu ska man ju egentligen göra något som är helt annorlunda, och det är det svåraste; alltså att bryta det gamla mönstret och komma in i det nya tänket. Nu har vi förvisso ett år på oss, men allt är samtidigt inte färdigdefinierat, för det är fortfarande mer information som vi behöver få in för att kunna sätta de exakta processerna. Och en bank har ju så många olika processer; Det är ju inte bara "vi köper något, och sedan säljer vi något", utan vi köper och säljer väldigt olika saker, och en sak som köps kan säljas på väldigt många olika sätt - och varje kombination är en enskild process. Så jag tror att dokumentationen av detta, för att sedan veta hur vi faktiskt ska jobba med det tar lite tid till - och sedan ska detta efterföljas enligt rutiner; det är det svåraste. Allt detta innebär en ny vardag och ett nytt arbetssätt för väldigt mycket olika saker. Så om vi kallar detta för "awareness" - för det är egentligen det detta handlar om; när vi vet hur en process ska skötas, hur saker och ting ska komma in i processen, och hur det ska lämna processen, så gäller det att veta att det faktiskt är så, och att det är det korrekta sättet att hantera det. Man kan liksom inte luta sig tillbaka och falla in i gamla mönster, för helt plötsligt uppenbarar sig en incident där.
IP3.31	H:	Men jobbar ni mycket med utbildningar angående denna "awareness"-biten?
IP3.32	M:	Ja, jag tycker det. Det blir liksom mycket fokus på det. Och projektet som sådant har ju tagit fram "akututbildningar", där man har gått ut och informerat. En utbildning är ju först och främst uppbyggd på grundlig information kring något. Nästa steg är ju mer att ge lite mer kött på benen, och specificera utbildningen till olika organisationsdelar för att det ska vara anpassat efter just deras verksamhet och arbetsuppgifter. Så det tycker jag vi gör ganska bra. I projektet så håller vi kontinuerligt på med utbildningar och information, både för projektdeltagarna men också resten utav företaget. Detta tills dess att det de riktiga utbildningarna är färdiga - istället för att vänta tills hela projektet är klart.
IP3.33	H:	Kör ni med interna utbildningar, eller tar ni in utomstående för att hålla utbildningarna?
IP3.34	M:	Ja, interna. Det finns inte så mycket som erbjuds från externt håll att vända sig till. De första generella utbildningarna om GDPR skulle ju vem som helst kunna hålla i, i princip. Men sen när det gäller mer specifik utbildning så är det ju något som är unikt för oss. Så man vill ju gärna omsätta det så att det är anpassat efter hur vi jobbar, tänker och efter våra utmaningar. Så, nej. Det är internt.
IP3.35	J:	**Okej. Vad skulle du då säga är receptet för att tackla denna utmaningen, alltså det processorienterade?**

IP3.36	M:	Att börja jobba enligt den processen som vi tänkt oss, och så tidigt som möjligt för att på så sätt få awareness-biten att sitta i ryggmärgen på ett tidigt stadie. Därmed måste ett antal nyckelpersoner i detta projektet eller på företaget måste ta på sig ambasadörsrollen. Och sedan gäller det hela tiden att övervaka arbetsuppgifterna så att ingenting bryter mot vad processerna säger. Skulle det hända så måste detta tas upp och diskuteras, så att alla hela tiden tänker på detta. Säkerhetstänket kring GDPR är ju egentligen ingenting nytt. Men många har kanske inte behövt tänka på det tidigare, fast nu gäller det alla. För vem som helst skulle kunna få för sig att skicka någonting, göra någonting, eller säga någonting som enligt den nya lagen innebär en incident - och därmed försätter företaget i en situation som innebär en stor risk. Så nu är det ju mycket mer allvar kring utbildningen av awareness-biten. Detta innebär också att alla måste ha tänket naturligt inom sig; om man ser någon som är ny, eller som helt enkelt inte tänker sig ordentligt för, så får man hålla koll på det - alla måste hjälpas åt att hålla koll på varandra. Det ska inte vara dumt att säga till någon, och informera dem när de gör fel. Utan då är det bättre att man förklarar för dem vad konsekvenserna av ett misstag kan innebära så att de förstår innebörden helt och hållit. Och jag menar; hellre det än att hålla varandra om ryggen, för förr eller senare kommer det ju fram att ett misstag har begåtts, och då är det bättre om det uppdagas så tidigt som möjligt. Sker det till exempel ett intrång som slår ner på flera företag, och då alla andra utom just Företag X har rapporterat detta när utredningen kommer, så skickar det signalerna att vi inte har koll, vilket i sin tur kan få förödande konsekvenser - för det är så många olika sätt det kan komma fram på med tanke på att alla företag kommer att ha så mycket mer koll.
IP3.37	J:	**Sista frågan angående processorientering; Vilka processorienterade förändringar har ni gjort, eller planerar ni att göra inom den närmsta tiden?**
IP3.38	M:	Vi har ju jobbat i processer länge, och många av de processerna vi kollar igenom nu kanske inte kommer att genomgå stora förändringar på pappret. Däremot, så tror jag att den del av de processerna som är dokumenterade inte längre stämmer, och att det därmed blir förändringar. Jag tror att att den största förändringen gällande processer - det är just incidenthantering. Detta i och med att vi inte gjort detta på denna nivån tidigare. Likadant gällande införande av förändringar och liknande. Den processen måste följas och det måste vara en process, inte flera olika. Så jag menar, det är mycket som är nytt och det är på en helt annan nivå dessutom: 0 till 100 på en gång, liksom. Så det är ju en stor uppförsbacke. Men samtidigt har Företag X resonerat som så; att nu tillsätter man helt nya roller och personer för ansvaret kring dessa processerna. Så det blir nytt för den personen och enklare att förhålla sig till än ifall denne varit tidigare anställd och arbetat med de gamla processerna.
IP3.39	H:	Så, dessa nya poster kommer bara att ansvara för de nya processerna?

IP3.40	M:	Ja, precis. Företag X har ju tidigt insett att vi kommer behöva helt nya personer och poster för dessa nya processer. Och då får dessa personer arbeta med det på heltid, istället för att man bara ger ytterligare ansvar till anställda som redan arbetar på 100% med sina respektive ansvarsuppgifter. IT kommer ju till exempel få en post som bara ansvarar för incidenthantering. Och det är ju en funktion av att läget blir mer kritiskt. Och allting hänger ihop; att köpa teknik är en sak. Men att få all teknik att hänga ihop med processerna som krävs är en helt ny utmaning, och då krävs det att det finns dedikerade personer som sköter detta. Sen vet jag ju många företag som inte jobbar i processer och inte har en aning om hur de ska göra. Och jag menar, det är bara ett år kvar innan lagen börjar gälla, så då är man sent ute om man inte kommit igång med arbetet ännu.
IP3.41	J:	Hur upplever du tidsaspekten med att det just nu bara är ett år kvar?
IP3.42	M:	Nä, men om man tar hänsyn till vilken nivå respektive bolag sätter - för det är lite diffust hur högt nivån ska ligga, och då handlar det mycket om: Ska det vara manuellt arbete? Hur mycket kraft ska vi lägga ner på att kontrollera att vi faktiskt jobbar som vi har skrivit, och enligt hur organisationen funkar? För det är det som allt handlar om. Det är en sak att göra det på pappret och anställa människor. Nästa steg är att få kontroll på att man faktiskt jobbar efter processerna, och att resurserna vi tagit in hinner med arbetsuppgifterna och så vidare. Övning helt enkelt. Man måste öva på GDPR; Iscensätta incidenter och mäta hur arbetet vid en incident då går och vilken tid det tar. Och det är vårt nästa steg framåt hösten. Vi har ju planerat en del scenario som ska övas, bland annat incident-biten, för den har vi flaggat hårt för. Och vi har ju tekniken, samt vi håller på med processerna, och personalen håller på att utbildas. Så jag är inte så orolig för att vi ska kunna arbeta in rutinerna på ett år. Däremot undrar jag hur myndigheterna ska kunna vara redo att göra kontroller tills GDPR träder i kraft. Jag har svårt att se att de skulle kunna vara klara att göra det nästa år. Det kan inte vara mer än en handfull företag som kommer att få en incident eller en kontroll på hur de jobbar. Min åsikt är att det kommer dröja tills 2019 innan alla företag kommer att få det svettigt, och få konkreta problem, så att säga
IP3.43	J:	**Näst sista frågan; Hur förhåller du dig till att GDPR, uttryckligen, förespråkar "Privacy by Design"?**
IP3.44	M:	Ja, det är väl bra att har ett begrepp att peka på och att det finns en dokumentation till viss nivå vad man menar med det. Men det är ganska luddigt. Det hade kanske varit bättre om man pekat på en viss standard: Att det ska vara en specifik nivå, det ska finnas den här, respektive den här funktion med i systemet etc. Med andra ord mer konkret. Privacy by Design handlar ju mycket om att göra rätt från början, men samtidigt, vad innebär det? Hur kontrollerar man kod? hur kontrollerar processer? hur kontrollerar man nya saker som förs in i systemet? Det säger ju inte Privacy by Design, och det tror jag många tycker är luddigt. De vill nog,

		tillsammans med mig ha lite mer konkreta exempel.
IP3.45	J:	Och hur känns det då att GDPR i artiklarna bara nämner "privacy by design", och inte sen definierar något mer precist vidare?
IP3.46	M:	Nä, men samtidigt är det ju väldigt svårt. Ska man nästa steg i en lag och vara så pass detaljerad, så kan det innebära att lagen måste skrivas om varje år - vilket heller inte är bra. Det gäller ju att hitta en balans mellan att tolkningsutrymmet. Det kan bli för öppet för tolkning, och samtidigt alldeles för snävt. Och i grunden tror jag att så länge man försökt tolka "privacy by design" så väl som möjligt och sedan gjort allt för att uppfylla detta, så tror jag att man som företag kommer att klara sig undan sanktioner. Så det är nödvändigt att det finns tolkningsutrymme. Ska man satsa på att 100% eftersträva GDPR på alla plan så hade man antagligen aldrig blivit färdig. Det kanske talar lite grann emot mig själv, men samtidigt, jag är en säkerhetskille; Jag sätter nivån för "Privacy by Design" mycket högre än vad kanske en ekonom hade gjort. "Privacy by Design" är ju inget nytt egentligen, utan det handlar bara om att säkerheten för ett system ska ha en väldigt hög lägsta nivå, så att säga. Och att arbeta proaktivt såklart.
IP3.47	J:	Har datainspektionen gett några direktiv angående Privacy by Design?
IP3.48	M:	Nä, inte vad jag vet. Jag vet bara att de sammanställt vanliga frågor på deras hemsida om hur de tolkar det osv. Mer än så vet jag faktiskt inte, så jag kan inte svara på det. Sedan tycker jag att vissa av de svaren på datainspektionens hemsida, tyvärr, är felaktiga och att tolkningarna är lite konstiga. Men samtidigt om en tekniker ställer en fråga angående deras ämnesområde och jurister från datainspektionen sedan ska ge ett svar - jag menar, hur bra kan det bli egentligen?
IP3.49	J:	**Nä, okej. Sista frågan: Hur ser du på en certifiering av gdpr, både från eget håll samt mot företag ni jobbar mot? För det står ju också uttryckligen i GDPR att man ska kunna få detta.**
IP3.50	M:	Jag hoppas bara man kontrollerar den certifieringen. Tanken är väll att det ska vara som vid PCI certifieringar - alltså Payment Card Industri - att man först får en stämpel för att man uppfyller kriterierna, men att de sedan också kommer ut - hur ofta vet jag inte - och kontrollerar att man faktiskt eftersträvar det och liknande. Precis som förr i tiden om man tittar på de som körde kvalitetssystem och liknande revisioner - även för ekonomi. Den typen av kontrollorgan tror jag är nödvändigt, och kan man då få internationella organ att gå ut och utbilda människor, gå ut och certifiera företag och sätta en stämpel, så kan de i sin tur säga att "vi är ju GDPR-ready". Då kan de per automatik få en enklare granskning när man ska göra affärer tillsammans. Istället för att man som företag ska behöva vara orolig och därmed själva behöva granska potentiella affärspartners. Detta är ju en stor fråga, för vi som bolag har ju ett ansvar idag att kontrollera våra partners; Kan ni garantera att ni hanterar

		information korrekt? Och då räcker det inte med att de bara skriver under på att det gör det. För missköter de sig så åker ju vi också på det. Därför kan en sådan certifiering försäkra oss om att det finns en tredje, och oberoende part som kontrollerar att de faktiskt efterföljer vad som skrivs under - vilket underlättar affärer, såklart. Så en tredje part som kontrollerar är definitivt att föredra. Och det är ju en konkurrenskraft också.
IP3.51	H:	Kommer ni att sikta mot en GDPR-certifiering?
IP3.52	M:	Det är inte sagt så. Eftersom att vi är en bank, och med tanke på att det finns en Europeisk bankförening, samt en Svensk bankförening som tittar på olika lagar och kommer med egna direktiv, så avvaktar vi vad resten utav bankerna säger. Det är möjligt att vi i slutändan skaffar en certifiering - vi får se. Vår förhoppning är ju att vi kommer att klara av GDPR. Först och främst handlar det ju om att ta sig över tröskeln att faktiskt klara det interna med GDPR.
IP3.53	J:	Okej, vi känner att det var allt vi hade och fråga om. Är det något utöver det vi frågat som du vill tillägga?
IP3.54	M:	Nää, faktiskt inte.
IP3.55	J:	Då tackar vi för oss och tack så mycket för intervjun!
IP3.56	M:	Tack själva.
IP3.57	J:	Vi skickar givetvis transkriberingen till dig senare så att du kan kontrollera att allt stämmer överens, och att inga felaktigheter finns med.
IP3.58	M:	Låter jättebra.

7.3.4 Företag Y

Bransch: Bank.

Intervjuperson: Magnus Svensson**.**

Yrkesroll: Projekt-/Programledare**.**

Tid och plats: 16.00-16.40, Måndagen den 8 maj 2017, möte i Helsingborg.

Referens nr.	Person:	Frågor och svar
IP4.1	J:	Godkänner du att vi spelar in intervjun?
IP4.2	M:	Ja, det är helt okej.
IP4.3	J:	Du har rätt att vara anonym - är detta något som du önskar?
IP4.4	M:	Nej, det är okej.
IP4.5	J:	**Okej. Då börjar vi med lite inledande frågor; Vad har du för tidigare bakgrund, dels akademiskt, men också yrkesmässigt?**
IP4.6	M:	Ja. Gällande akademiska studier så är jag civilekonom - tre år av ekonomiska studier - med inriktning marknadsföring. Sen har jag en tvåårig magisterprogram i kommunikation. Det är min bakgrund. Sen efter det har jag jobbat fyra år uppe på Ideon i projektledarroll, och sedan regionchef - en affärsplanstävling. Därefter har jag jobbat på bank i lite olika roller; Fältsäljare, kontorschef, projektledare och de tre senaste åren har jag jobbat som management konsult - vilket jag gör idag också.
IP4.7	J:	**Okej. vilken roll har du idag på Företag Y?**
IP4.8	M:	Projektledare, eller kanske snarare programledare för ett GDPR-program.
IP4.9	J:	**Alright. Hur skulle du säga att verksamheten idag arbetar för att tillmötesgåendet mot GDPR?**
IP4.10	M:	Mm. Då tycker jag att man gjorde en väldigt klok sak här på företag y. I min roll som konsult, så möter vi väldigt många av våra existerande kunder, men också väldigt många nya kunder. Och på de allra flesta ställen så pratar de om GDPR - de flesta är rädda för GDPR tack vare de höga böterna. Oftast är det då IT eller Legal som är drivande i detta hos ett företag. Men, man kommer inte loss därför att ingen äger det fullt ut. Så det blir som någon slags Linje-amöba som vandrar runt mellan olika enheter, och så händer det egentligen ingenting. Men det man gjorde väldigt klokt på företag y, det var att man startade ett program. Helt enkelt att man bröt det loss från linjen, och så satte man ett ansvar på

		det. Och den här gången valde man att sätta det på en extern aktör för att hålla ihop programmet - vilket då blev jag från Do-Be Consulting tillsammans med två andra konsulter. Men det mest relevanta i denna goda hanteringen, var att bryta det fritt och lägga det som ett program, samt att sätta ett ansvar på det. Till detta, kopplades en styrgrupp - alltså allt det här man gör med ett program; Man ger det en egen budget, man ger det en tidsplan, man ger det en leveranspalett. Och detta tror jag är en av nyckelfaktorerna med GDPR, därför att man mäktar inte med det i en roll som linjechef att göra det ensam. Likaså skulle inte Legal mäkta med att driva det själv.
IP4.11	J:	Just därför att de redan har en heltidsroll i sin nuvarande arbetsuppgift?
IP4.12	M:	Ja, absolut. Man är ju anställd för att ha en arbetsuppgift, och i denna arbetsuppgift så jobbar man ju förhoppningsvis runt 100%. Och GDPR kräver ju då ytterligare 100%. Så det går inte att driva det själv helt enkelt - det krävs med andra ord en ny roll för att driva, leda, och hålla ihop programmet. Så det skulle jag säga är det absolut klokaste som företag y gjorde - alltså att driva det fritt. Och detta tycker jag att alla organisationer borde göra.
IP4.13	J:	**Okej. Hur stort skulle du säga att förändringsarbetet är - hur många system berörs?**
IP4.14	M:	Här är vi nere på 189 system som berörs. Men man kan samtidigt inte säga att det bara gäller system. Utan, GDPR handlar ju om att ha koll på personuppgifter i hela företaget. Och då kan man titta på det ur många olika perspektiv; Är systemen hanterar personuppgifter compliant? Men sedan har man ju en artikel i förordningen som säger att alla behandlingar också ska vara kartlagda. Och ser man det istället utifrån behandlingsperspektivet, så berörs ju varje enhet inom företaget dessutom. Exempelvis ekonomienheten, business support-enheten, säljenheten och finansenheten. I alla dessa olika enheter så sker ju olika typer av behandlingar. Och i samtliga måste man ha koll på: Vad är behandlingen, vilket syfte har den, och vilken legal grund har vi på den? Sedan vidare: Gör vi behandlingen för att fullfölja kontrakt? Gör vi det för ett legitimt intresse? eller är det på grund av ett legalt krav? Så på så sätt är det svårt att säga hur stor omfattningen är - förutom att den är just väldigt stor. Men det går inte att definiera omfattningen i antal system.
IP4.15	J:	Aha, nä för att man också exempelvis kan räkna det i humankapital?
IP4.16	M:	Precis. Man kan ju också definiera omfattningen, precis som du säger, som i en kulturförflyttning av en organisation: Hur du som organisation, och som enskild individ i organisationen ställer dig till hanteringen av GDPRs principer i det dagliga arbetet. Det skulle jag nästan säga vara det största. I och med att man inte har haft något jätte-bestraffande regelverk tidigare, i kombination med att Sverige haft den s.k. Missbruksregeln som undantag, så har man kunnat hantera

		personuppgifter lite som man vill: Man har kunnat ta ut excel-listor på det man vill, samt skickat personuppgifter mellan varandra inom organisationen. Men nu måste man ju göra en kulturförflyttning där man hela tiden tänker till i det vardagliga arbetet; ”Oj, här har jag en uppgift som är en personuppgift, då måste jag ju faktiskt tänkte på principerna: Jag får inte lov att skicka den hur som helst, jag måste skydda den, och jag måste ta bort den efter en viss tid”. Och så vidare. Detta är ju en jättestor utmaning.
IP4.17	J:	**Okej. Så vi går över till de tekniska utmaningarna. Vad skulle du säga vara den största utmaningen, rent tekniskt, gällande tillmötesgåendet mot GDPR?**
IP4.18	M:	Det skulle jag säga vara Data Breach - och allt vad som ingår med detta. ”Rätten med att bli glömd”, och pseudonymisering/Anonymisering. Men nu talar jag i och för sig inte utifrån vad som direkt ingår i min arbetsroll. Utan jag talar för vad jag hör andra uppleva som den största utmaningen. En sak att lägga till är ju den här artikeln om ostrukturerad data - det som missbruksregeln täckt upp för. Beroende på hur man väljer att tolka denna, så känns det som att inget företag kommer att kunna bedriva sin verksamhet längre. Alltså, får man inte maila personuppgifter liksom? Jag förstår inte den helt ut faktiskt. Men angående ”rätten att bli glömd”: Det känns rätt klurigt att se till att detta följs i 189 system.
IP4.19	J:	**Okej. Vad skulle du då säga vara den rätta vägen för att tackla dessa utmaningar?**
IP4.20	M:	Vi gör dels en beskrivning av varje system, där vi har en process som bygger på att vi identifierar systemet. Sedan har vi en Data Gathering där vi samlar in och klär datan utifrån GDPR - Vad för data har vi, och hur länge ska vi spara datan osv. Sedan gör vi en GDPR-analys, där man tittar på detta och försöker se vilka konsekvenser som kan tillkomma. Efter det går denna analysen till IT så de i sin tur får bedöma den. Då är det upp till dem att ta reda på vad de skulle kunna göra, samt vilka aktiviteter som ska införas för att göra respektive system GDPR-compliant. Därefter tas det ett beslut med alla stakeholders involverade: Antingen blir det då en IT-task som läggs i den ordinarie agila verksamheten - inplanerat i sprintarna. Alternativt blir lösningen bli processförbättringar. Vi som ett program bildar ett projekt kring allt; IT driver sina uppgifter och vi gör våra. Så det är det ena, att vi med den processen tittar på varje system. Sen driver vi även det här arbetet om att titta på behandlingar på respektive enhet: Och där genomkör vi arbetsmöten med respektive enhet för att försöka få fram deras olika behandlingar. Ställ frågan en gång till så ska jag försöka förtydliga det hela.
IP4.21	J:	Ja, alltså rätta vägen för att tackla dessa tekniska utmaningar?

IP4.22	M:	Precis. Det som har kommit fram i båda dessa strömmarna är ju egentligen att de rättigheterna som kunderna har: ”Rätten att bli glömd”, ”Rätten att få korrekta uppgifter” osv. Dessa går inte att lägga på systemnivå. Det går inte att implementera rättigheterna i varje system. Utan där måste vi titta på generella tjänster. Så då kommer vi driva tillsammans med IT där vi förklarar för dem angående respektive område. För det blir för mycket att implementera detta på varje system. Nu är ju jag ingen IT-människa, men det blir kort sagt generella lösningar som ligger ovanför varje system, så att säga.
IP4.23	J:	**Okej. Vilka tekniska förändringar har ni gjort, eller planerar ni just nu att göra för att detta ska uppfyllas?**
IP4.24	M:	Just nu är åtta system inne i utvecklingsfas, men det är ju av totalt 189 - så det är ju en del kvar. Men det man märker på det som planeras in i sprintarna, så är det mycket som rör dataminimeringskravet. Det vill säga, när tar vi bort data? Hur tar vi bort data? Men även, vem kommer åt datan? Vi har ju en tidsplan för varje system, så när det har blivit ett beslutsmöte och vi har satt igång IT-aktiviteterna, så kommer det att vara full fart hela vägen fram till att det är klart - förhoppningsvis februari.
IP4.25	H:	**Vi glömde en fråga tidigare som vi tänkte ta nu. Hur många består av program-gruppen av?**
IP4.26	M:	Ungefär 15-20 personer som, på olika arbetstimmar, är involverade.
IP4.27	J:	**Okej. Då går vi över till det processorienterade perspektivet; Vilka är de största utmaningarna gällande tillmötesgåendet mot GDPR, rent processorienterat?**
IP4.28	M:	Change Management, och Data Breach igen faktiskt. Om jag börjar med Data Breach; Att svara upp mot de 72 timmarna baserat på vilket systemstöd vi har. Där har vi än så länge inte tagit några beslut. Vi vet att regleringen finns. En i gruppen skriver policys om huruvida vi ska titta på det och hur vi ska tänka kring det. Därefter kommer vi skriva ett beslutsunderlag som egentligen ska hantera allt om vilken ambitionsnivå av GDPR vi ska ha; Ska vi köpa in fyra system som övervakar allt och ser till att vi inte får Data Breaches? Eller kommer vi gå in på mer manuella lösningar - om det inträffar en incident så har vi en grupp som vet vi exakt hur vi ska agera i olika scenarion? Där det lite delade meningar. En del förespråkar ett starkt systemstöd för att upptäcka och hantera data breaches, medan andra aktörer menar att den manuella lösningen i olika arbetsgrupper är bättre. Jag tror ändå att det kommer bli en ganska så jobbig process att ta sig igenom. Dels för att det finns olika ambitionsnivåer, och dels för att det innebär en omfattande arbete som ska tas fram när det väl inträffar - för att det är känsligt. Så data breach tror jag är en processmässig jobbig aktivitet att sätta i organisationen. Sedan gällande Change Management, som tangerar det som ni antagligen kallar ”Privacy by Design”. Det finns ganska bra flöden i de

		flesta organisationer för IT-utveckling. Men GDPR påverkar ju allting som handlar om personuppgifter - så det kan också vara processförbättring det handlar om. Att sätta en process i en organisation som hanterar alla initiativ - det kommer bli kämpigt, fast det är samtidigt väldigt bra. Att få alla intressenter att skriva under på detta, och sen att faktiskt genomföra det utan en massa undantag.
IP4.29	J:	**Okej. Vad skulle du då säga är det bästa receptet för att tackla dessa processorienterade utmaningarna med Data Breach, och Change Management?**
IP4.30	M:	Det är egentligen klassiskt; att börja med att rita upp processen och sedan inkludera alla som är med i den. Alltså, Processinriktat arbete som utgår ifrån: vilka delprocesser ingår? Vilka överlämningspunkter har vi - för det är ofta där det skiter sig. Och var är startbehovet, respektive slutbehovet, för att sedan titta på det och ta med alla som arbetar i det. För då kan du egentligen inte göra så mycket fel. Så det blir tvär-funktionella grupper som jobbar med operationalisering av policys där personer från olika enheter ska ingå för att täcka upp allt. Alltså, viktiga stakeholders som är involverade i processen - antingen som intressent eller aktör. Jag tror inte då att det kommer sättas under ett och samma, utan snarare workshop-serie helt enkelt. Detta med god facilitator och metod för att kunna genomföra allt.
IP4.31	H:	Kommer ni testa olika case av en incident exempelvis, som träning alltså?
IP4.32	M:	Ja men absolut. Alltså, en processbeskrivning är ju en teoretisk beskrivning utav verkligheten - det är ju vad en processbeskrivning är. Men sedan ska det ju köras också, och då kanske det uppstår andra problem, så det är absolut så att vi kommer att göra det. Men vi är ju väldigt långt ifrån den fasen egentligen, även om det har börjat lite grann - vilket i och för sig är bra.
IP4.33	J:	**Okej. Vilka processorienterade förändringar har ni genomfört, eller planerar ni att genomföra just nu?**
IP4.34	M:	Jag ska ta fram min dator, för det finns faktiskt nedskrivet.
IP4.35	J:	Ja, kanon.
IP4.36	M:	Men det är ju då baserat på Legals analys utav GDPR, och utifrån det tagit fram vilka policys som måste uppdateras och vilka processer som påverkas, så att säga.. ett ögonblick så ska jag få igång min dator.
IP4.37	H:	Under tiden tänkte jag ställa en fråga. Jag tänkte på det med att du sade att ni hade 8 system som just nu höll på aktivt med; Har ni analyserat alla system redan och sedan bara börjat på dessa, eller analyserar ni efter hand?

IP4.38	M:	Jag tror att det är så att vi har 30 system som är prioriterade. Det vill säga kärnsystem som stödjer bankens huvudprocesser - de viktigaste helt enkelt. Så då börjar vi med dem. Men det finns fortfarande system som fortfarande ligger i identifierings-fasen - vi vet att de finns men har inte klätt dem med data ännu. Så nej, vi har inte analyserat alla system ännu.
IP4.39	H:	Okej.
IP4.40	M:	Så, nu ska vi se. Här kommer det som vi planerar att genomföra:
IP4.41	M:	- ”Procedure for right to be informed of change purpose”: det vill säga om vi ändrar syftet med en behandling av personuppgift. ● ”Procedure for right to rectification”. ● ”Procedure for deletion - right to be forgotten”. ● ”Procedure for right to restriction of processing”: Det vill säga att invända mot att vi behandlar data. ● ”Procedure for notification of restriction of processing erasure or rectification”. ● ”Procedure for data portability and right to access”. ● ”Procedure for right to object” ● ”Procedure for DPO” ● ”Procedure for change management”: Alltså, Privacy de Design. ● ”Procedure for contracting”. ● ”Procedure for Data Breach”. ● ”Procedure for documentation of processes and systems”. ● ”HR Procedures”. Det är dem som vi har på papper i dagsläget.
IP4.42	H:	Som ni håller på att förändra?
IP4.43	M:	Nej, utan de ligger i planeringen. För först ska policys skrivas för dem, och det är inte gjort ännu på grund av sjukdom av den ansvarige. De skulle varit klara i april. Så det har skjutits upp. Planen var också att genomföra fyra stycken innan sommaren inom ”right to be informed of change purposes”. Det vill säga: ”Procedure for right to object”, ”Procedure for DPO”, ”Procedure for change management” och ”Procedure for Data breach”. Så att vi kunde börja jobba med dem nu innan sommaren, och sedan resterade efter sommaren. Men vi får se helt enkelt. Med andra ord, inte genomfört någonting ännu.
IP4.44	J:	**Och nu till allmänt om GDPR; Hur förhåller du dig till att GDPR, uttryckligen, förespråkar ”Privacy by Design”?**
IP4.45	M:	Jag är ju en sådan person som gillar struktur. Och jag tycker att det är väldigt bra för företag, oavsett bransch, att det finns en struktur som hanterar hur man genomför förändringar. Vilket gör att ”Privacy by Design” är fantastiskt bra gällande att det finns ett regelverk som säger åt ett företag att man måste ta med personuppgiftsbehandlingar när man

		planerar att utveckla ny systemvara eller nya processer. Det tvingar liksom företag att få in tänket och utvecklingen i ett flöde. Vissa kanske tycker att det är ”fyrkantigt”, men jag tycker att det är bra.
IP4.46	J:	Menar du att det är bra att det tvingar systemen att hålla en högre standard?
IP4.47	M:	Ja, men precis. Delvis att det blir en standard, men också att det blir ett krav på dig som företag på att du måste sätta upp checklistor eller en beställningsprocess som svarar upp mot lagen. Det låter kanske lite flummigt. Men ”Privacy by Design” innebär ju att du som bolag måste tolka det, du måste säga ”Vad innebär detta för oss?”, och så måste du fatta beslutet om ”Okej, hur hanterar vi detta då?”. Och den hanteringen tror jag blir att många företag kommer sätta en produktutvecklings-process där dessa kraven kommer in som en naturlig del. Vilket jag tror är bra, för då finns det ingen som kan köra vid sidan om och utveckla sitt eget, utan allt det blir i ett flöde. Och det tycker jag är väldigt positivt. Sedan tror jag det fortfarande det krävs ganska så mycket tolkning om vad det innebär, men jag tycker ändå det är positivt.
IP4.48	H:	Hur långt har ni kommit med programmet? När planerar ni att vara färdiga?
IP4.49	M:	Vi har ju ett mål, och det är att vi ska vara compliant, med definitionen utifrån besluten som fattas inom programmet, exempelvis data breach kan ju läggas på olika nivåer. Men det är ju i maj 2018. Sen kommer ju förvisso olika delar av programmet vara klart vid olika tidpunkter. Men programmet kommer ju inte stängas förrän i juni-juli kanske. Och då stänga det med en tydlig överlämning till en ny DPO-organisation, som lever vidare med det här och ser till att processerna efterlevs och att man arbetar enligt dem. Det måste uppföljningar så att alla tänker på principerna i dagligt arbete, och alla vet hur alla rapporteringar ska gå till, samt alla vet var riktlinjer styrdokument finns. Alltså, allt som levererats används och så vidare - en kulturförflyttning helt enkelt.
IP4.50	H:	Hur ska ni då se till att detta genomförs?
IP4.51	M:	Utbildningar och kommunikation. Det är en utav arbetsströmmarna i programmet, och det är jag som leder den arbetsströmmen. Så det som vi har löpande är då att vi sätter upp en struktur för att kommunicera, det vill säga, vi äger en egen del utav intranätet som bara handlar om GDPR. Där skickar vi ut nyhetsbrev varje månad. Vi har också en FAQ samt en mail-adress där man kan skicka in frågor som sedan besvaras och läggs på i FAQn. Så det är kommunikationsdelen. Sedan när det gäller utbildningar så har vi börjat uppifrån och ner egentligen; Så vi har börjat med utbildningar för ledningsgruppen. Just nu kör vi Business Area Meetings, det vill säga utbildningar för olika mellanchefer, kan man säga, och informerar kortfattat om GDPR, vad det innebär för banken och hur vi bedriver programmet. Sedan kommer vi gå ännu djupare,

		framåt höst och vinter, då vi kommer att gå in på vad det innebär för en ”vanlig”, eller ”gemene man” anställd på företaget, så att säga - Olika nivåer på utbildningar helt enkelt. I samband med detta mäter vi kunskapen nu innan i form utav frågor till alla. Sedan är tanken att vi ska mäta kunskapsnivån igen framåt nästa vår, där förhoppningen är att vi kommer att se en generell ökad kunskap och medvetenhet angående GDPR för alla i organisationen.
IP4.52	J:	**Okej. Sista frågan är hur du ser på de certifieringsmekanismerna som GDPR, uttryckligen, beskriver? Hur tänker du kring dessa?**
IP4.53	M:	Jag är lite för lite insatt i dem. Men jag hoppas och tror att certifieringen kommer knytas väldigt nära ISO-standarder. Jag tror inte de kan leva olika liv, utan jag tror att man måste titta på ”okej, vad säger olika ISO-standarder?”. Och är det då någon liten del som inte redan omfattas av dem - för mycket finns ju redan på olika sätt inom andra ISO-standarder. Men det är klart, det är alltid positivt med certifiering, rent proportionellt sett. Men jag passar nog på den frågan, för jag är lite för dåligt insatt om dem.
IP4.54	J:	Det är helt okej. Är det någonting du vill tillägga?
IP4.55	M:	Nä, faktiskt inte.
IP4.56	J:	Okej, då tackar vi så mycket för intervjun. Vi skickar givetvis en transkribering av intervjun till dig, så att du kan kontrollera att det stämmer överens med vad du menat och så vidare.
IP4.57	M:	Det låter bra! Tack själva.

Referenser

Cavoukian, A., 2010. Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph. D. *Identity in the Information Society*, *3*(2), ss. 247-251. http://link.springer.com/article/10.1007/s12394-010-0062-y
[2017-04-13]

Datainspektionen, 2017a. *Introduktion till dataskyddsförordningen.* http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/dataskyddsdagen/
[2017-03-30]

Datainspektionen, 2017b. *Allmänna frågor - om EU:s dataskyddsreform.* http://www.datainspektionen.se/fragor-och-svar/eus-dataskyddsreform/allmanna-fragor/#A4
[2017-03-30]

Datainspektionen, 2017c. *Anmälningar av personuppgiftsincidenter.* http://www.datainspektionen.se/fragor-och-svar/eus-dataskyddsreform/anmalningar-av-personuppgiftsincidenter/
[2017-03-30]

Datainspektionen, 2017d. *Förberedelser inför EU:s dataskyddsförordning - vägledning till personuppgiftsansvariga.* http://www.datainspektionen.se/Documents/vagledning-forberedelser-pua.pdf
[2017-03-30]

Datainspektionen, 2017e. *Personuppgiftsansvarig – Vem är personuppgiftsansvarig* http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/personuppgiftsansvarig/
[2017-04-10]

Datainspektionen, 2017f. Personuppgiftsansvarig – Personuppgiftsbiträde. http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/personuppgiftsansvarig/
[2017-04-10]

Datainspektionen, 2017g. Dataskyddsombud. http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/skyldigheter-for-de-som-behandlar-personuppgifter/dataskyddsombud/
[2017-04-21]

Datainspektionen, 2017h. *Förberedelser för personuppgiftsansvariga.* http://www.datainspektionen.se/dataskyddsreformen/forberedelser/forberedelser-for-personuppgiftsansvariga/

[2017-04-20]

Datainspektionen, 2017i. *Missbruksregeln upphör.*
http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/missbruksregeln-upphor/
[2017-04-20]

Datainspektionen, 2017j. *Rätt till information.*
http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registrerades-rattigheter/ratt-till-information/
[2017-04-20]

Datainspektionen, 2017k. Dataportabilitet.
http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registrerades-rattigheter/dataportabilitet/
[2017-04-21]

Dimentional Research, 2016. *GDPR: Perceptions and Readiness. A Global Survey of Data Privacy Professionals at companies with European Customers.*

Europaparlamentets och rådets direktiv 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119/1,4.5.2016).
http://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679&rid=1
[2017-04-11]

Gürses, S., Troncoso, C. and Diaz, C., 2011. Engineering privacy by design. *Computers, Privacy & Data Protection*, *14*(3).
https://software.imdea.org/~carmela.troncoso/papers/Gurses-CPDP11.pdf
[2017-04-13]

Hammer, M, Champy, J, & Svensson, P 1994, *Reengineering The Corporation : Ett Radikalt Nyskapande Av Processer För Att Uppnå Dramatiska Resultatförbättringar I Organisationen*, n.p.: Göteborg : ISL (Institutet för säljträning och ledarutveckling), cop. 1994 ; (Uddevalla : Media print), Library catalogue (Lovisa), EBSCO*host*, viewed 23 May 2017.

Jacobsen, D I (2002). *Vad, hur och varför: om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen,* Lund, Studentlitteratur.

Kung, A., Freytag, J.C. and Kargl, F., 2011. Privacy-by-design in ITS applications. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a* (ss. 1-6). IEEE.

http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5986166&tag=1
[2017-04-13]

Moran, J.W. and Brightman, B.K., 2000. Leading organizational change. *Journal of Workplace Learning*, *12*(2), ss. 66-74.
http://www.emeraldinsight.com/doi/pdfplus/10.1108/13665620010316226
[2017-04-23]

Paton, R.A. and McCalman, J., (2008). *Change management: A guide to effective implementation*. Sage.
http://ebookcentral.proquest.com/lib/lund/reader.action?docID=880860
[2017-04-23]

Schaar, P., 2010. *Privacy by design*. Identity in the Information Society, 3(2), ss .267-274.
http://link.springer.com/article/10.1007/s12394-010-0055-x
[2017-04-13]

SFS 1998:204. Personuppgiftslag.

Rodrigues, R., Barnard-Wills, D., De Hert, P., & Papakonstantinou, V., 2016. *The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR*. *International Review of Law, Computers & Technology*, *30*(3), 248-270.
http://www.tandfonline.com/doi/abs/10.1080/13600869.2016.1189737
[2017-04-25]

Rodrigues, R, Wright, D, & Wadhwa, K 2013,'Developing a privacy seal scheme (that works)', *International Data Privacy Law,* 3, 2, p. 100, Supplemental Index, EBSCO*host*, viewed 23 May 2017.
http://resolver.ebscohost.com/openurl?sid=EBSCO%3aedo&genre=article&issn=20443994&ISBN=&volume=3&issue=2&date=20130501&spage=100&pages=100-100&title=International+Data+Privacy+Law&atitle=Developing+a+privacy+seal+scheme+(that+works)&aulast=Rodrigues%2c+Rowena&id=DOI%3a&site=ftf-live
[2017-04-23]

Tankard, C 2016,'Feature: What the GDPR means for businesses', *Network Security*, 2016, pp 5-8, ScienceDirect, EBSCO*host*, viewed 23 May 2017.
http://ac.els-cdn.com/S1353485816300563/1-s2.0-S1353485816300563-main.pdf?_tid=1c492624-4054-11e7-b5b8-00000aacb35f&acdnat=1495611745_3987aa68a097a66927f0c783f5c42e29
[2017-04-15]

Todnem By, R., (2005). Organisational change management: A critical review. *Journal of change management*, *5*(4), ss. 369-380. http://www.tandfonline.com/doi/full/10.1080/14697010500359250?scroll=top&needAccess=true
[2017-04-23]