LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Förändringsarbetet mot GDPR

Upplevda utmaningar i arbetet mot efterlevnad av den nya dataskyddsförordningen

Kandidatuppsats 15 hp, kurs SYSK16 i Informationssystem

Författare: Jens Andersson
Edward von Essen

Handledare: Umberto Fiaccadori

Examinatorer: Björn Svensson
Benjamin Weaver

Förarbetet mot GDPR: Upplevda utmaningar i arbetet mot efterlevnad av den nya dataskyddsförordningen

FÖRFATTARE: Jens Andersson och Edward von Essen

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

FRAMLAGD: maj, 2018

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 61

NYCKELORD: GDPR, Dataskyddsförordningen, Change Management, Organisationsförändring, Ledarskap, PUL

SAMMANFATTNING (MAX. 200 ORD):
Under de senaste åren har insamling och lagring av data ökat drastiskt, samtidigt som personlig integritet och behandling av personliga uppgifter blivit allt viktigare frågor för allmänheten. Den tidigare lagstigningen gällande detta har inte förmodat att hänga med i denna utveckling, vilket resulterat i att en ny dataskyddsförordning kommer träda i kraft den 25:e maj 2018 och ersätta de nationella personuppgiftlagarna bland de europeiska medlemsländerna. Det nya direktivet, GDPR, syftar likt föregående direktiv till att stärka individers personliga integritet, med nya krav på hur organisationer skall behandla uppgifter som ett resultat av den tekniska utvecklingen. Detta innebär en del omfattande förändringar för de organisationer som behandlar personuppgifter. Denna studie är ämnad att undersöka vilka organisatoriska utmaningar GDPR-ansvariga anser är problematiska vid slutskedet av förändringsarbetet mot den nya dataskyddsförordningen, samt hur dessa problem hanteras. En kvalitativ undersökning har genomförts i form av fyra intervjuer med GDPR-ansvariga som alla har god kompetens inom området. Resultatet visar på att organisationer står inför en del organisatoriska utmaningar där efterlevnad, ledarskap och attityd hos såväl kund och anställda har stor påverkan.

Innehållsförteckning

Tabeller

1 Introduktion

I mars 2018 uppmärksammades det för världen att dataanalys bolaget Cambridge Analytica hade samlat personlig information från upp till 50 miljoner Facebookanvändare (Solon & Laughland, 2018). Datorer, mobila enheter och molntjänster har fått en alltmer central roll i samhället och på grund av den snabba tekniska utvecklingen samlas och lagras data om människor i allt större utsträckning än tidigare.

I dagsläget anses data vara en av de mest värdefulla tillgångarna som verksamheter besitter och utnyttjar (IBM, n.d). Trots detta lagrar verksamheter stora mängder data i form av personuppgifter som de inte har någon nytta av eller som saknar ändamål (Davenport & Prusak, 2000). Facebook-Cambridge är bara en av flera skandaler som har uppmärksammat diskussionen kring personlig integritet och insamling av personliga uppgifter.

Sedan 1998 har personuppgiftslagen (PUL) behandlat frågor relaterade till personlig integritet på internet i Sverige och fungerat som en stöttepelare för hur personlig information från individer får nyttjas (Datainspektionen, 2018a). Personuppgiftslagen ämnar att skydda den personliga integriteten för varje EU-medborgare och i varje medlemsstat (Datainspektionen, 2018a). Lagen bygger på EU:s tidigare dataskyddsdirektiv från 1995 och har låtit varje enskilt EU-land få skapa sin egen tolkning av direktivet (Datainspektionen, 2018a).

Med den snabba tekniska utvecklingen har ytterligare krav ställts på hur personuppgifter skall behandlas, lagras och tolkas. På grund av detta kommer ett nytt datadirektiv träda i kraft den 25:e maj 2018. De nationella tolkningarna av EU:s gamla datadirektiv kommer att ersättas av en ny förordning; GDPR eller dataskyddsförordningen vars ändamål är att tydliggöra hur hantering och insamling av personliga uppgifter och data ska hanteras och lagras (Datainspektionen, 2018b). Det nya direktivet kommer att ge individer större inflytande över hur deras personliga information används samtidigt som verksamheter måste påvisa hur dessa uppgifter används, hanteras, lagras och till vilket ändamål (Datainspektionen, 2018b).

Enligt en undersökning från den multinationella advokatbyrån Baker & McKenzie (2016), där 110 personer från olika organisationer deltog, var många organisationer oförberedda på nya lagen och cirka 45 % av respondenterna i undersökningen indikerade att de inte hade verktygen för att säkerställa att deras organisation uppfyller de viktigaste kraven enligt GDPR.

1.1 Problemområde

Införandet av GDPR är den mest omfattande förändringen av integritetsförordningar på flera decennier och kommer att påverka alla företag som i någon form hanterar personuppgifter. I PuL har man tidigare kunnat behandla personuppgifter i ostrukturerat material med hjälp av missbruksregeln och låtit hanteringen av personuppgifter i ostrukturerat material utföras

någorlunda fritt så länge det inte har ansetts kränkande (Datainspektionen 2018a). Vid situationer där man upplever att ett brott har begåtts har man i varje enskilt fall gjort en bedömning om ett eventuellt övertramp har skett (Datainspektionen, 2018c). I den rådande lagstiftningen kan organisationer enligt personuppgiftslagen bli bötfällda på ett mindre belopp och betala skadestånd till de personer som blivit utsatta för bristande personuppgiftsbehandling. Den nuvarande lagstiftningen har alltså varken resulterat i särskilt stora legala eller ekonomiska konsekvenser för företag som har varit bristande i deras personuppgiftshantering.

Till skillnad från föregående lagstiftning kommer samtliga företag som i någon form behandlar personuppgifter i enlighet med GDPR bli skyldiga till att rapportera om en eventuell personuppgiftsincident sker. Om en organisation utsätts för dataintrång eller förlorar kontroll över personuppgifter är de enligt Datainspektionen skyldiga att rapportera detta inom 72 timmar till tillsynsmyndigheten och till de individer som berörs.

Som incitament för att företag skall följa de nya reglerna tillkommer höga sanktionsavgifter för de verksamheter som inte uppfyller de krav som GDPR medför. Om en verksamhet inte överensstämmer med stadgarna kan de bli bötfällda på 20 miljoner euro eller 4 % av företagets globala intäkter (Datainspektionen, 2018b), vilket förutsätter att verksamheterna noga identifierar och genomför de organisationsförändringar som krävs för att möta de satta kraven enligt den nya dataskyddsförordningen (Goddard, 2017).

Det har gått över två år sedan Europaparlamentet annonserade att den nya dataskyddsförordningen skall träda i kraft 25:e maj 2018 och det är inte lång tid kvar tills de måste ha uppfyllt de krav som den nya förordningen ställer. År 2016 visade Baker & Mckenzies (2016) undersökning att många organisationer var oförberedda på den nya dataskyddsreformen. I nuläget är de företag som påverkas av förordningen i slutskedet av sitt förändringsarbete som ska vara klart den 25:e maj. Då överträdelse av förordningen kan resultera i höga sanktionsavgifter om inte kraven uppfylls, är det kritiskt för organisationer att se över de verksamhetsprocesser som kommer att påverkas.

1.2 Forskningsfråga

Utifrån det formulerade problemet har vi valt att utgå från nedanstående frågeställning. Denna frågeställning syftar främst till att få ökad förståelse och kunskap om vilka utmaningar som GDPR-ansvariga anser är problematiska vid införandet av den nya dataskyddsförordningen.

- Vilka organisatoriska utmaningar anser GDPR-ansvariga är problematiska med förändringsarbetet inför den nya dataskyddsförordningen och hur går de tillväga för att lösa dessa utmaningar?

1.3 Syfte

Syftet med studien är att identifiera och redogöra för de organisatoriska utmaningar GDPR-ansvariga anser är problematiska vid införandet av den nya dataskyddsförordningen. Vidare ämnar studien att undersöka hur de går tillväga för att ta sig an dessa utmaningar. Genom att

belysa och undersöka vad som upplevs som problematiskt, och förstå hur organisationerna försöker hantera problemen framskymtar en förståelse för det omfång och det ansvar som de ansvariga för GDPR-anpassningen lever under i slutskedet av förarbetet.

1.4 Avgränsningar

- Vi kommer inte att tolka dataskyddsförordningen GDPR utan istället basera studien på datainspektionens tolkning av den.

- Vi undersöker de organisatoriska utmaningar som anses problematiska innan införandet har ägt rum och ämnar inte att undersöka vilka utmaningar som kan uppstå efter införandet.

- Studien syftar inte till att föreslå lämpliga lösningar, utan kommer endast identifiera upplevda utmaningarna och hur de hanteras av organisationerna.

- Studien kommer inte vara inriktad på tekniska utmaningar men kommer inte heller att bortse från dem.

1.5 Centrala begrepp

Datainspektionen - En svensk myndighet vars uppgift är att skydda människor mot att deras personliga integritet kränks genom felaktig behandling av dessa uppgifter.

Dataskyddsreformen - EU:s nya förordning för hur personuppgifter om EU-medborgare skall behandlas och lagras för att stärka den enskilde medborgarens integritet. Förordningen kommer stå över de nationellt stiftade lagarna och gäller i alla EU-länder.

PUL - Sveriges rådande lagstiftning för behandling av personuppgifter. Personuppgiftslagen syftar till att skydda den personliga integriteten hos privatpersoner och bygger på ett EU-direktiv från 1998.

Organisation - En organisation består av en grupp människor som tillsammans verkar för att nå gemensamma mål. Exempel på detta är myndigheter eller bolag.

Change management - En kollektiv term för de tillvägagångssätt som används för att förbereda individer och organisationer inför en organisationsförändring.

2 Litteraturgenomgång

I litteraturgenomgången beskrivs den teori som är relevant för studien. Litteraturgenomgången är uppdelad i två delar. Först presenteras teori som är relevant för att få en förståelse för rådande lagar och den kommande lagstiftningen GDPR. Den andra delen behandlar hur organisationsförändring påverkar verksamheter och framgångsfaktorer som kan bidra till ett lyckat förändringsarbete. Teorin som har tagits fram grundar sig i akademiska artiklar med olika infallsvinklar som är kopplade till området.

2.1 Definition av lagen

2.1.1 Personuppgiftslagen

Personuppgiftslagen (PUL) är Sveriges tolkning av EU:s datalagringsdirektiv från 1995 och trädde i kraft 1998 (Datainspektionen, 2018a). Enligt Datainspektionen (2018a) syftar PUL till att skydda människor från att deras personliga integritet kränks vid behandling av personuppgifter och reglerar hur personuppgifter får hanteras. Datainspektionen (2018a) definierar *behandling* som insamling, lagring, registrering, bearbetning mm. I personuppgiftslagen skiljer man på personuppgifter i strukturerat och ostrukturerat material (Datainspektionen, 2018c). Strukturerat material är data som lagras i traditionella dataregister, databaser och ärende- och dokumenthanteringssystem. Ostrukturerat material är personuppgifter som behandlas i löpande text, E-mail, ljud och bild (Datainspektionen, 2018c). Datainspektionen (2018d) definierar en personuppgift som följande:

> *"All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet räknas enligt personuppgiftslagen som personuppgifter. Även bilder (foton) och -ljudupptagningar på individer som behandlas i dator kan vara personuppgifter även om inga namn nämns. Krypterade uppgifter och olika slags elektroniska identiteter, som exempelvis IP-nummer, räknas som personuppgifter om de kan kopplas till fysiska personer."*

2.1.2 General Data Protection Regulation

Den allmänna dataskyddsförordningen (GDPR) kommer att ersätta personuppgiftslagen i Sverige och har som syfte att standardisera dataskyddslagstiftningen i alla 28 EU-länder genom att införa striktare stadgor för kontroll och behandling av personligt identifierbar information. Det nya direktivet utökar skyddet av personuppgifter och kommer att ge varje EU-medborgare större inflytande över hur deras personuppgifter hanteras (Datainspektionen, 2018b).

Direktivet står över alla nationella personuppgiftslagar som inte ämnar att stärka den personliga integriteten (Eu.riksdagen, 2018). Fastän huvudprinciperna för dataintegritet fortfarande är relativt lik föregående direktiv, som personuppgiftslagen (PuL) är baserad på, tillkommer nya krav som organisationer måste ta hänsyn till (Datainspektionen, 2018b). Exempel på sådana krav är anmälan om dataintrång, inbjudan om samtycke och ansvar för

dataöverföring utanför EU. Om dessa krav inte uppfylls riskerar de verksamheter som behandlar personuppgifter att behöva betala sanktionsavgifter (Datainspektionen, 2018b).

2.2 Förändringar som förordningen kommer att medföra

Både personuppgiftsansvarig (PuA) och personuppgiftsbiträde (PuB) blev ursprungligen myntade i personuppgiftslagen, vilka kommer kvarstå även med den nya förordningen, med ett antal nya krav.

2.2.1 Personuppgiftsansvarig

Enligt datainspektionen (2018e) är en personuppgiftsansvarig (PuA) den organisation eller myndighet som beslutar om behandling, gallring och sparande av personuppgifter samt hur detta skall gå till. En personuppgiftsansvarig kan vara en fysisk person som ansvarar för att behandlingen av uppgifter stämmer överens med dataskyddsförordningens stadgar (Datainspektionen, 2018e). Personal får endast bearbeta uppgifter i överensstämmelse med personuppgiftsansvariges instruktioner (Datainspektionen, 2018e). Vidare har denne ett ansvar att genomföra organisatoriska och tekniska åtgärder för att kunna redovisa att behandlingen av personuppgifter sker enligt dataskyddsförordningens lagstadgar. Detta kan redovisas med certifieringar och uppförandekoder (Datainspektionen, 2018e).

2.2.2 Personuppgiftsbiträde

Personuppgiftsbiträde (PuB) är den som på uppdrag av personuppgiftsansvarig gallrar, sparar och behandlar personuppgifter (Datainspektionen, 2018f). Denna person är extern och arbetar utanför organisationen som den personuppgiftsansvarige befinner sig på (Datainspektionen, 2018f). Ett personuppgiftsbiträde kan vara en juridisk person, institution, myndighet eller annat organ som enligt instruktioner från personuppgiftsansvarig får behandla personuppgifter. Enligt Datainspektionen (2018f) har personuppgiftsbiträdet precis som den personuppgiftsansvarige ansvar för att föra register över hantering, utse ett dataskyddsombud och säkerställa att man håller lämplig säkerhetsnivå. För att samarbete mellan PuA och PuB skall ske måste ett personbiträdesavtal upprättas (Datainspektionen, 2018f).

2.2.3 PuB-avtal

I samband med att GDPR träder i kraft måste organisationer enligt datainspektionen (2018g) ansvara för att både personuppgiftsansvarig och personuppgiftsbiträde skall tillsättas. När ett sådant samarbete inrättas krävs det att ett skriftligt PuB-avtal med personuppgiftsbiträdet upprättas (Datainspektionen, 2018g). Avtalet innehåller de punkter som personuppgiftsbiträdet måste ta på sig och innefattar bland annat att denne endast får hantera uppgifter enligt instruktioner från personuppgiftsansvarig samt bistår den personuppgiftsansvarige med relevant information för att visa på att man uppfyller alla skyldigheter som biträde (Datainspektionen, 2018g)

Brook (2018) menar på att förändringsarbetet mot GDPR-arbeten fokuserar mycket på att se över leverantörskontrakt eftersom GDPR förändrar förhållningssättet kring transparens och

tillgänglighet av personliga uppgifter. Detta är främst för att säkerställa att de processer som tillhandahålls av tredjeparter också skall stämma överens med de nya kraven. Vidare hävdar Brook (2018) att det är många leverantörer som använder kontraktsmallar som inte är uppdaterade, vilket är en risk när GDPR träder i kraft eftersom gapen inte kommer att vara uppdaterade i tid.

2.2.4 Förordningens punkter

Tillgänglighet
Alla individer kommer från och med den 25 maj 2018 ha rätt att ta del av de personuppgifter som organisationer har registrerat om dem. Det är även varje enskilt företags ansvar att se till att denna information distribueras på rätt sätt (Datainspektionen 2018h).

Spårbarhet
Organisationer måste ha tydlig dokumentation och resonemang om var, varför och hur data lagras och behandlas. Personuppgiftsansvarig (PuA) och personuppgiftsbiträdet (PuB) är enligt lag skyldiga att föra register över hur personuppgifterna behandlas. Dessa register skall vara skriftliga eller i elektroniskt format (Datainspektionen, 2018i).

Transparens
Varje enskild individ skall ha rätt till att få ut information om hur dennes personuppgifter hanteras (Datainspektionen, 2018e). Denna information skall lämnas över av personuppgiftsansvarig både när personuppgifterna samlas in och när den registrerade individen begär detta (Datainspektionen, 2018e).

Korrigering
Varje enskild individ har rätten att vända sig till en organisation som behandlar dess personuppgifter för att få felaktiga personuppgifter om dem korrigerade. Detta innebär även att individen i fråga har rätten att komplettera med uppgifter som saknas och som anses relevanta med avseende till ändamålet med uppgiftsbehandlingen (Datainspektionen, 2018j).

Rätten att bli bortglömd
Varje individ skall ha rätten att vända sig till en verksamhet som behandlar dess personuppgifter för att be om att få uppgifterna raderade. Detta gäller om uppgifterna inte längre används i det syfte som de samlades in för, om individen återkallar samtycket, om behandlingen används i direktmarknadsföring eller om individen motsätter sig i hur uppgifterna behandlas (Datainspektionen, 2018k).

Portabilitet
I vissa fall kommer den som lämnat sina personuppgifter ha rätten att få sina dem förflyttade till en annan organisation eller myndighet. Data som begärs ut skall utlämnas i ett allmänt och maskinläsbart format (Datainspektionen, 2018l).

2.3 Organisationsförändring

2.3.1 Change Management

En kollektiv term för att skapa förståelse för organisationsförändring är Change management (Todnem By, 2005). Todnem By (2005) definierar Change management som processen som jämt förnyar en verksamhets riktning, struktur och färdighet att tillgodose de växlande behoven hos såväl externa som interna faktorer. Organisationsförändringar kan se olika ut beroende på situation och verksamheters olikheter (Burnes, 2009). Därför är det viktigt för organisationer att kunna identifiera hur de bedriver den nuvarande verksamheten samt hur de vill se ut i framtiden eftersom förändring ständigt är närvarande på både ett strategisk och operativ plan (Burnes, 2009). En organisationsförändring kan till exempel innebära omorganisering, implementation av ny teknologi eller införandet av nya lagar och förordningar (Anderson & Anderson, 2002).

Todnem By (2005) hävdar att 70 procent av alla förändringsprogram misslyckas på grund av bristande ramverk och strategier för hur en förändringsprocess skall hanteras. Vidare argumenterar hon att den forskning som har publicerats inom ramen för organisationsförändring innehåller lite bevis för vilka nyckelfaktorer som avgör hur en framgångsrik förändringsprocess skall genomföras (Todnem By, 2005). Burnes (2009) förklarar att det finns två faktorer som man kan enas om. Den första är att förändringar på den rådande marknaden sker i en allt snabbare takt än tidigare. Den andra är att förändring kan komma från såväl interna som externa faktorer och i alla former. Anderson och Anderson (2002) beskriver i sin bok om förändringsprocesserna Transitional change och Transformational change.

Transitional change är projekt med tydliga start -och slutdatum som innefattar betydande förändringar i miljön som organisationen verkar i (Gilley, McMillan, & Gilley, 2009). Istället för att förbättra något som redan finns i organisationen handlar transitional change om att ersätta en verksamhetsfunktion med en helt annan (Anderson & Anderson, 2002). Vanligtvis uppstår transitional change när ledningen identifierar ett problem eller när en existerande funktion inom organisationen behöver utvecklas eller bytas ut (Gilley et al., 2009). Exempel på sådana processer är vid omorganisering, när nya policys införs eller vid implementation av nya system som inte kräver storartade förändringar i attityder och beteenden (Gilley et al., 2009). Om ledningen får problem med kulturella och mänskliga faktorer i Transitional change beror det oftast på att medarbetare känner sig osäkra på vad som skall göras eller att förarbetet med den nya implementationen är illa planerad (Anderson & Anderson, 2002).

Transformation change är den mest komplexa typen av förändring som organisationer kan gå igenom (Anderson & Anderson, 2002). Denna förändringstyp handlar i enkelhet om att styra organisationen från ett tillstånd till ett helt annat, så nytt tillstånd att man behöver göra förändringar i organisationskulturen, beteenden, tankegångar och uppehålla denna förändring över tid (Anderson & Anderson, 2002). Transformational change kräver att man ändrar medvetenheten och de anställdas syn på världen, deras arbete samt dess kunder. Detta är något som även Moran och Brightman (2000) är tydliga med att framföra. De påstår att det är viktigt att personen som leder förändringsarbetet skall förstå varför förändringen är nödvändig för organisationen och hur de på ett effektivt sätt skall kunna genomföra förändringen i enlighet med organisationens affärsmål (Moran & Brightman, 2000).

2.3.2 Ledning vid organisationsförändring

Ett starkt ledarskap skall identifiera vilken väg organisationen avser att gå, vilka nuvarande begränsningar som finns samt vilka resurser som behövs för att effektivt genomföra förändringen (Chapman, 2002). Ett sådant tillvägagångssätt anser Smith (2005) kan innebära att man aktivt visar på de avvikelser som finns mellan det nuvarande tillståndet och det önskade tillståndet. Det har i flera akademiska rapporter diskuterats om hur man bör gå tillväga för att ta sig an förändringsarbeten. Under fyra decennier observerade Dr. Kotter organisationer för att se hur de gick tillväga för att genomföra sina strategier och förändringar. Efter att ha observerat olika organisationer identifierade han åtta framgångsfaktorer som han menade att organisationer bör ta hänsyn till för att lyckas med en omfattande förändring (Kotter, 1995).

Den första punkten handlar om att *upprätta en känsla av att det är brådskande.* Kotter (1995) anser att det en fördel om hela organisationen förstår varför förändringen är nödvändig och att man i ett tidigt skede skapa en känsla av att förändringen är viktig för organisationen. Detta i sin tur gör det lättare för organisationen att motivera personal att genomföra den (Kotter, 1995). Smith (2005) förklarar även att första steget inom förändring är att förmedla att det är nödvändigt att ändra "status quo" (Smith, 2015).

Det andra steget handlar om *att forma en kraftfull och vägledande* grupp. För att övertyga de anställda till att förändringen är nödvändigt krävs ett starkt ledarskap (Kotter, 1995). Clarke (1999) menar att projekt kan ha tydliga mål, men innehåller alltid osäkerheter då varje projekt är unikt. Ofta kan det vara svårt att definiera vilka mål man avser att uppfylla, hur lång tid det kommer att ta samt hur mycket det kommer att kosta (Clarke, 1999). Att bilda en grupp människor som leder arbetet är enligt Kotter (1995) en viktig faktor för att kunna genomföra förändringsarbetet på ett effektivt sätt. Denna grupp bör bestå av rätt människor med olika kompetensområden som har ett stort inflytande och förtroende inom organisationen (Kotter, 1995).

Det tredje steget handlar om att *ta fram en tydlig vision* som återspeglar vad förändringen ska uppnå och motivationer till att åtgärderna som tas fram går mot rätt riktning (Kotter, 1995). Därför är det i detta steg viktigt att ta fram strategier som kan vara till hjälp för att kunna genomföra visionen (Kotter, 1995).

Det fjärde steget handlar om att visionen eller förändringen bör kommuniceras frekvent och på ett kraftfullt sätt genom att påvisa förändringens syfte och mål. Vad du gör med visionen och hur du förmedlar den till andra kommer att påverka hur framgångsrik förändringen kommer bli (Kotter, 1995). Detta bör även göras på ett enkelt sätt och genom olika kommunikationskanaler (Kotter, 1995).

Det femte steget handlar om *att hjälpa andra att agera på visionen*. För att kunna genomföra visionen krävs det enligt Kotter (1995) att man tar bort de hinder som är i vägen för förändring. Detta kan innebära att ändra befintliga system eller strukturer som inte ligger i linje med visionen (Kotter, 1995). Att identifiera personer som är negativt inställda till förändring och hjälpa dem se vilket värde och varför förändringen behövs anser Kotter (1995) är väsentligt för att genomföra en lyckad förändring. Detta bekräftas även av Weiner (2009) som förklarar att en effektiv förändringsprocess bör ses som en lagsport, men att det ofta uppkommer problem när vissa känner sig engagerade i genomförandet men andra inte gör det.

Effektiviteten blir högre när människor har en känsla av förtroende och kollektivt kan genomföra organisationsförändringarna (Weiner, 2009).

Det sjätte steget handlar om *skapa kortsiktiga vinster* vilket enligt Kotter (1995) är viktigt för att bibehålla motivationen och att skapa ett stort förtroende för visionen. Genom att framföra delmål kan man motivera personalen till att förändringen är positiv (Kotter, 1995).

Det sjunde steget handlar om att *befästa vilka förbättringar som har gjorts* och hur man kan fortsätta anpassa strukturer så att de uppfyller förändringsvisionen. Kotter (1995) hävdar att omfattande förändringar tar lång tid och att många förändringsprojekt misslyckas eftersom man tar ut segern i förskott. Att ständigt analysera vad som går bra och vad som behöver förbättras är ett viktigt steg.

Det sista steget handlar om att man skall *etablera de nya tillvägagångssätten* och se till förändringen att bli en del av kärnan av organisationen och organisationskulturen (Kotter 1995). Schneider, Brief, & Guzzo (1996) menar även att ledarens förmåga att förankra förändringsarbetet i företagskulturen är en viktig del för att uppnå ett framgångsrikt förändringsresultat.

2.3.3 Attityder vid organisationsförändring

Begreppet företagskultur beskriver vilka gemensamma värderingar och beteendemönster som finns inom en organisation (Schneider et al., 1996). Anledningen till att så många organisationsförändringar leder till motstånd är organisationens bristande förmåga på att visa att en förändring kommer att ske (Jones, Jimmieson, & Griffiths, 2005). Enligt Schneider et al. (1996) och Smith (2005) innebär organisationsförändring till stor del att hantera de människor som påverkas under processens gång och att många förändringsarbeten tidigare har misslyckats på grund av att människor inom organisationerna inte har accepterat förändringen.

Det finns många faktorer som påverkar effektiviteten vid organisatoriska förändringar. Armenakis, Harris & Mossholder (1993) presenterar begreppet Readiness for change som en av dessa faktorer. Denna faktor handskas med organisationens alla involverades attityder, övertygelser och åsikter med avseende på hur stora förändringar som behöver göras och organisationens förmåga att framgångsrikt utföra dessa förändringar (Armenakis et al., 1993). Armenakis et al. (1993) berättar att energi, inspiration och stöd måste komma inifrån organisationen och att dessa faktorer är viktiga byggstenar om man vill skapa förståelse för förändring.

Jones et al. (2005) anser att anställda som får ta del av högkvalitativ information om de förändringar som skall äga rum sannolikt även kommer att vara mer tillmötesgående. I samband med detta menar Puhakainen och Siponen (2010) att utbildning är en av de viktigaste aspekterna för att bli effektiv i sin förändringsprocess och för att uppnå efterlevnad vid införandet av nya policys. Utbildning är en viktig del eftersom organisationen på så sätt kan aktivera de anställdas tankegångar och ge dem en förståelse för varför det är viktigt att följa de nya reglerna (Puhakainen & Siponen, 2010). Om en anställd dessutom får intrycket av att ledningen involverar sig i förändringen kan benägenheten bli större att bemöta den information som krävs för att tillmötesgå den nya förordningen eller policyn (Hu, Dinev, Hart, & Cooke, 2012).

2.4 Problematiken med nya lagar och policys

Puhakainen och Siponen (2010) förklarar att det finns en stor oro inom organisationer att anställda inte engagerar sig när nya säkerhetspolicys införs. I fallet med den nya dataskyddsförordningen är detta speciellt allvarligt då företag riskerar att betala upp till 4 % av den globala omsättningen eller 20 miljoner euro om de inte följer de riktlinjer som den nya dataskyddsförordningen medför (Datainspektionen, 2018b).

För att tillmötesgå komplexa lagar och förordningar krävs det kunskap och förståelse men om en organisation inte besitter denna kunskap kan de inte tydligt identifiera vad som utgör en lagöverträdelse (Mendoza, Dekker, & Wielhouwer, 2016). Detta bekräftas även av Otto och Anton (2007) som berättar att det kan vara mycket utmanande att arbeta med nya juridiska texter eftersom de innehåller många korsreferenser, tvetydigheter och akronymer som ofta ändras efter nya regler och rättspraxis. Mendoza et al. (2016) förklarar att regelverk ofta är beroende av andra vägledande dokument som är till för att hjälpa läsaren att förstå och tillämpa lagen. Dessa typer av kompletterande dokument innehåller vanligtvis tidigare administrerade rättsavgöranden, referenser och handböcker för hur lagen skall tolkas (Mendoza et al., 2016). Finns det inte tydliga dokument eller referenser till övriga dokument som krävs för att förstå lagen finns det även risk att lagen misstolkas (Otto & Anton, 2007).

Vidare menar författarna att informationssäkerhet och datasekretesslagar fortfarande är framväxande områden och att det därför förekommer större variation i dessa lagars krav (Otto & Anton, 2007). Detta beror på att reglerna inom området är relativt nya och därför finns det mycket lite rättspraxis för att vägleda organisationer i hur lagen skall appliceras (Otto & Anton, 2007). Den nya dataskyddsförordningen är ett exempel på detta, eftersom lagen inte har satts i bruk finns det inga prejudikat att luta sig mot. Komplexa lagar som inte har någon rådande rättspraxis kan resultera i en negativ inverkan på efterlevnad eftersom det blir svårare för organisationer att förstå och tillämpa reglerna (Mendoza et al., 2016). För att underlätta förståelsen anser Mendoza et al. (2016) att verksamheter kan dra nytta av att investera i utbildning av anställda eller ta in extern hjälp i form av experter och konsulter inom området.

2.5 Teoretisk översiktstabell

Nedan visas de centrala delarna som har redovisats i litteraturgenomgången. Dessa har sammanställts i en tabell tillsammans där det även redogörs vad respektive område avser att undersöka. Tabellen är sammanställd för att ge läsaren en tydlig överblick över resultaten som har hittats i litteraturgenomgången.

Tabell 1: Teoretisk översiktstabell.

Kategori	**Teori/Referens**	**Undersöker**
Definition av lagen	**Personuppgiftslagen** (Datainspektionen, 2018)	Nuvarande lag kring personuppgiftshantering samt vad den nya dataskyddsförordningen

	General Data Protection Regulation (Datainspektionen, 2018) **Förordningens påverkan på företag och privatpersoner** (Datainspektionen, 2018)	kommer ställa för krav på organisationer.
Organisationsförändring	**Change management** (Todnem By, 2005)**,** (Burnes, 2009)**,** (Anderson & Anderson, 2002)**,** (Gilley, McMillan, & Gilley, 2009)**, (**Moran & Brightman, 2000) **Ledning vid organisationsförändring** (Chapman, 2002), (Smith, 2005), (Kotter, 1995), (Clarke, 1999), (Weiner, 2009), (Schneider, Brief, & Guzzo, 1996) **Attityder vid organisationsförändring** (Schneider, Brief, & Guzzo, 1996)**,** (Jones, Jimmieson, & Griffiths, 2005)**,** (Smith, 2005)**, (**Armenakis, Harris & Mossholder, 1993), (Puhakainen och Siponen, 2010)**,** (Hu, Dinev, Hart, & Cooke, 2012)	Begreppet samt olika typer av organisationsförändringar och vad dessa innebär. Vikten av att ha en stark ledning vid förändringsarbete samt framgångsfaktorer för att uppnå ett effektivt förändringsresultat. Vikten av god företagskultur samt hur människors attityder kan både främja och motverka ett förändringsarbete.
Problematiken med nya lagar och policys	(Puhakainen och Siponen, 2010), (Mendoza, Dekker, & Wielhouwer, 2016), (Otto & Anton, 2007)	Problematiken med införandet av nya lagar samt hur dessa faktorer påverkar förändringsarbetet.

3 Metod

I detta kapitel beskrivs och motiveras vilka metoder som har använts samt hur undersökningen genomförts. Därtill presenteras respektive informant som har givit empiri till studien samt varför deras kompetens är relevant för undersökningen. Avslutningsvis framförs det vilka tillvägagångssätt som har använts för att öka studiens kvalitet genom att diskutera uppsatsens validitet, reliabilitet, etik samt hur urvalet ser ut. Målet är att ge läsaren en inblick i hur studien har utförts för att öka trovärdigheten.

3.1 Metodval

Denna studie har en explorativ problemställning vilket har styrt metodvalet mot en kvalitativ datainsamling. Jacobsen (2002) menar på att en explorativ problemställning ofta kräver en metod som går på djupet och nyanserar i form av intervjuer för att få fram kvalitativa data. Denna undersökning kräver ett metodval som resulterar i att många olika aspekter lyfts fram, Jacobsen (2002) anser då att en kvalitativ ansats att föredra framför en kvantitativ ansats. Den kvalitativa metoden lägger tonvikten på närhet som ett mycket viktigt element i strävan att förstå människors uppfattning av verkligheten (Jacobsen, 2002).

3.2 Intervjuer

Den vanligaste metoden för datainsamling inom det som kallas kvalitativ metod är öppna intervjuer. Jacobsen (2002) anser att det är större chans att få ett givande samtal vid en besöksintervju än vid en telefonintervju. Därför har vi valt att genomföra alla våra intervjuer ansikte mot ansikte. Detta eftersom det lättare skapas en förtrolig stämning om man fysiskt sitter i samma rum. Besöksintervjuer bidrar även till mindre begränsningar i vad uppgiftslämnaren kan säga till skillnad från telefonintervjuer (Jacobsen, 2002).

Inom metodlitteraturen skiljer man ofta mellan två grupper av intervjuplatser: naturlig och konstlad (Jacobsen, 2002). En naturlig plats är en omgivning som intervjuobjektet är välbekant med. En konstlad plats är en omgivning som intervjuobjektet inte är familjär med. Forskning har visat att den miljö som intervjun sker i påverkar innehållet och att en konstlad miljö kan bidra till att intervjuobjektet ger konstlade svar (Jacobsen, 2002). Därför togs beslutet att hålla samtliga intervjuerna på informanternas företag.

Vi valde att spela in alla intervjuer med hjälp av en applikation på mobiltelefonen. Fördelen med detta tillvägagångssätt är att vi kan undvika att anteckna under intervjuns gång och istället upprätthålla en naturlig dialog med de som vi intervjuar, vilket även Jacobsen (2002) förespråkar. Genom att ha god ögonkontakt och inskränka anteckningar får man intervjun att flyta på bättre och kan dessutom få direkta och ordagranna citat, vilket är en fördel då det ger rapporten extra tyngd (Jacobsen, 2002). Vissa kan reagera negativt på inspelningar och blir nervösa när de får veta att intervjun skall spelas in. För att skapa en så avslappnad och naturlig dialog som möjligt frågade vi i god tid innan om intervjun fick spelas in och gjorde klart att både personen i fråga och organisationerna de representerade var anonyma.

3.2.1 Intervjuguide

Till grund för intervjuerna använde vi oss av vår intervjuguide (Tabell 2). Intervjuguiden innehåller frågor som är relevanta för att få fram information om de problemområden som behandlas i teorin. Jacobsen (2002) anser att en intervju utan en viss struktur riskerar att resultera i att viktiga ämnen glöms bort. Dock kan en intervju med för hög struktur resultera i att den kvalitativa ansatsen minskar. Intervjuguiden har därför fungerat som ett hjälpmedel för att hålla en öppen dialog men samtidigt säkerställt att områden som är relevanta för undersökningen inte glömts bort. Vidare har den även varit till hjälp för att undvika att beröra områden som inte är av relevans.

3.2.2 Bearbetning & Analys av data

Efter intervjuerna transkriberades innehållet och analyserades för att få en överblick över den insamlade informationen. Den data som intervjuerna framställde låg till grund för analysen och diskussionen där teorin sedan har kopplats.

Analys av kvalitativa data grundar sig i tre kärnområden; Beskrivning, systematisering och kategorisering samt kombination. Beskrivningsfasen syftar till att få en så detaljerad och grundlig beskrivning av vår data. I nästa fas har vi systematiserat och reducerat oöverskådliga data genom att sålla och förenkla information för att få en överblick av de problemområden som fanns. När detta var gjort började vi tolka informationen genom att generalisera, hitta meningar och samband samt få i ordning datan. Jacobsen (2002) belyser hur viktiga dessa steg är för att inte riskera att utelämna relevant information i undersökningen.

3.2.3 Informanter

Tabell 2: Informanter.

Informant 1 - I1 **Genomförd** 2018-04-17 **Samtalslängd** 29:58 **Transkriberade ord:** 3034	**Roll** Director of technology. Leder GDPR arbetet internt. Jobbar även med GDPR åt kunder. **Organisation – O1** IT - konsultbolag. <1500, >1000 anställda **Relevant erfarenhet** Teknikchef inom Region syds avdelning på O1. Arbetat med datasäkerhet i över 5 år och med GDPR i 1.5 år.
Informant 2 - I2 **Genomförd** 2018-04-17 **Samtalslängd** 31:52 **Transkriberade ord:** 4051	**Roll** Junior Konsult. GDPR ansvarig internt och arbetar även med GDPR åt ett stort världsledande företag. **Organisation – O2** IT - konsultbolag. <1500, >1000 anställda **Relevant erfarenhet** Utbildning hos Datainspektionen. Jobbat med GDPR i ett år.
Informant 3 - I3 **Genomförd** 2018-04-25 **Samtalslängd** 36:52 **Transkriberade ord:** 3896	**Roll** Projektledare för arbetet med GDPR internt. **Organisation - O3** Offentlig sektor. >30 000 anställda. **Relevant erfarenhet** Arbetat med informationsstyrning de senaste 5 åren. Projektledare för GDPR-arbetet sen juni 2017.
Informant 4 - I4 **Genomförd** 2018-05-08 **Samtalslängd** 29:55 **Transkriberade ord:** 2228	**Roll** IT-service managementkonsult. Ansvarig för GDPR-arbetet både internt och hos kund. **Organisation -O4** It-bolag som erbjuder heltäckande lösningar inom IT-infrastruktur. >2000 anställda. **Relevant erfarenhet** Lång erfarenhet av informationshantering och informationssäkerhet.

3.3 Urval

I undersökningen användes ett ändamålsenligt urval där vi riktade förfrågan till de som vi antog kunde ge oss utförliga och kvalitativa svar. I urvalsprocessen satte vi upp ett kriterium; att intervjuobjekten ska vara ansvariga för arbetet med GDPR internt eller jobba med GDPR som konsulter. Av intervjuobjekten arbetar tre som konsulter med GDPR-arbetet både internt och ute hos kund. Den fjärde är ansvarig projektledare för GDPR-arbetet internt. Innan kontakt inleddes identifierades ca 30 organisationer som vi ansåg vara relevanta. Dessa baserades på geografisk närhet, tillgänglighet samt på kriteriet som är nämnt ovan.

Eftersom GDPR snarts träder i kraft är det många GDPR-ansvariga som har mycket att göra och därför blev vi avvisade av några av de förfrågade. Vi bestämde oss dock för att hålla oss inom ramen för de intervjuobjekt som vi trodde kunde ge oss kvalitativa svar och fick slutligen kontakt med fyra personer att intervjua. Eftersom arbetet med den nya förordningen är i sitt slutskede valde vi att inte begränsa urvalet inom en specifik bransch, även om majoriteten av intervjuobjekten arbetar inom IT-sektorn.

Kontakt med intervjuobjekten fördes främst via mail. I mailet presenterades det att vi var ämnade att undersöka vilka organisatoriska utmaningar som ansågs problematiska vid införandet av den nya dataskyddsförordningen och hur de arbetar för att tillmötesgå dessa. Vi redogjorde att vi var studenter på Lunds universitet som skriver kandidatuppsats inom ämnet för GDPR. Utifrån svaren om tänkbar medverkan bestämdes plats och tid med de fyra personer för intervjuerna som ligger till grund för insamlingen av empirin. Jacobsen (2002) menar att anonymisering minskar risken för att intervjuobjekten ska tala osanning. Vi har därför valt att anonymisera alla namn och organisationer i vår undersökning. I tabell 2 är intervjupersonerna sammanställda.

3.4 Validitet & Reliabilitet

Orden validitet och reliabilitet används för att avgöra värdet av empirin som samlas in (Jacobsen, 2002). Med validitet menas att empirin måste vara giltig och relevant. För att säkerställa empirins relevans, så består intervjuguiden av en blandning av öppna och konkreta frågor. Vi strävade efter att ha så öppna frågor som möjligt men ansåg och att det är intressant för undersökningen hur organisationerna ser på vissa konkreta problemområden som arbetet med GDPR har medfört. För att stärka studiens validitet har vi skickat transkriberingen från intervjuerna till respektive informant. Detta för att säkerställa att transkriberingen är korrekt genomförd och för att ge informanterna en möjlighet att korrigera eventuella felaktigheter.

Tre av fyra av våra informanter är verksamma som konsulter i IT-branschen och har delat med sig av sina erfarenheter från både intern- och kundperspektiv. Detta gör att resultatet kan generaliseras på andra branscher. En del av syftet med studien är att identifiera problemområden, vilket kräver att informanterna vågar erkänna egna brister och tillkortakommanden. För att motverka detta har vi varit tydliga med att dem, deras företag och deras kunder är anonyma.

3.5 Etik

Under vår undersökning har vi utgått från Jacobsens (2002) tre etiska aspekter. Dessa är informerat samtycke, rätt till privatliv och krav till att bli korrekt framförd. Informerat samtycke innebär att den som deltar i undersökningen gör det frivilligt och är medveten om vilka risker och vinster ett deltagande medför (Jacobsen 2002).

I några fall har den initiala kontakten varit via en @infomail vilket gör att vi inte kan garantera att det inte har funnits några påtryckningar från chefer eller dylikt. Detta är dock inget vi har upplevt då samtliga respondenter har varit positiva till intervjuerna. I korrespondensen med informanterna har vi varit tydliga med syftet med undersökningen och har meddelat respondenterna i förväg om vad intervjun kommer att handla om. Detta har gjorts genom att innan intervjun gett dem tillgång till en kort beskrivning av vårt problemområde och vår intervjuguide. Innan varje intervju har vi frågat och fått ett godkännande att spela in intervjun. Därefter har samtliga intervjuer har transkriberats och hittas under rubriken bilagor. Transkriberingen har förmedlats till respektive respondent för att säkerställa att den information som återges är korrekt.

3.6 Kritik av metodval

Nackdelen med att använda sig av kvalitativ undersökning är att man inte kan samla in lika mycket data från informanter som vid en kvalitativ undersökning. Vi märkte dessutom att perspektiven och antalet nya poänger minskade vid den fjärde intervjun, vilket även Jacobsen (2002) menar är vanligt när man använder sig av öppna intervjuer.

4 Resultat

I resultatdelen presenteras sammanställningen av empirin från samtliga intervjuer. För att hålla den röda tråden har empirin utgått från rubrikerna i den teoretiska översiktstabellen och kommer att presenteras i löpande text. Vi kommer även att behandla organisatoriska utmaningar som informanterna upplever som inte går under dessa rubriker.

4.1 Organisationsförändring

4.1.1 Ledning vid organisationsförändring

På frågan om ledningen aktivt är med och förankrar arbetet inför GDPR inom organisationen svarade både informant 1, 2 och 4 att ledningen internt gör det, men att det har varit problematiskt ute hos kund. Informant 2 berättar att ledningen hos de företagen han arbetar hos har olika förhållningssätt i arbetet med den nya dataskyddsförordningen. För att tydliggöra berättar han om hur attityden hos ledningen faller inom tre olika nivåer.

> *"Det finns låg nivå, medelnivå och hög nivå. Låg nivå kopplas ofta till personer som tror att den nya förordningen kommer att hamna mellan stolarna och att det är en grej som kommer och ingen bryr sig om det. Medelnivå är att man försöker förhålla sig till förordningen och försöker förstå sig på vad man bör göra för att vara safe. Då är det oftast att man gör sårbarhetsanalyser samt går igenom och reviderar Pub-avtal och vanliga avtal. När man kommer på hög nivå så är det att man börjar analysera på processnivå. Då försöker man analysera den processen eller subprocessen för att se vad man ska plocka bort för att inte komma i kontakt med personuppgifter [...]."(Informant 1, 2018)*

Informant 2 anser att majoriteten av företagen som de är i kontakt med idag ligger på en låg-medelnivå. Vidare berättar informanten att den nivån ledningen lägger sig på sjunker nedåt och avgör vilken nivå som organisationen hamnar på.

> *"Det som ledning tar beslut för och vilken nivå ledningen lägger sig på sjunker ju nedåt." (Informant 2, 2018)*

Informant 3 menar att det är problematiskt att inte ledningen internt är med och förankrar de nya riktlinjerna och tillvägagångssätten de anser sig behöva inför GDPR så att det får fäste inom organisationen. På frågan om ledningen aktivt arbetar med att förmedla hur man bör arbeta svarar informant 3:

> *"Nä det gör dom inte. Dom har utsett projektet då. Projektet har problem att nå uppåt." (Informant 3, 2018)*

Informant 3 menar att bristen på förståelse hos ledningen bidrar till att det inte tillsätts tillräckligt med resurser.

> *"[…] Man har verkligen inte fokuserat och tagit det här på allvar innan. Så det är*

> *vår största utmaning nu att faktiskt få den nya organisationen att förstå hur mycket resurser en verksamhet med 12 tusen anställda behöver." (Informant 3, 2018)*

Informant 1 berättar att utmaningen för dem har legat i att bolagen tidigare har varit decentraliserade i den bemärkelsen att varje region har varit relativt fristående från resterande regioner i bolaget. Vidare berättar informant 1 att de olika regionerna har varit isolerade från varandra när det gäller policys, riktlinjer och liknande. Eftersom GDPR slår på hela koncernen berättar både informant 1 och 4 att den nya förordningen har tvingat dem till att samarbeta inom hela koncernen för att följa samma vision.

> *"Men i och med att det här slår på en koncernnivå så måste koncernen ta ett helhetsgrepp på väldigt stora bitar av GDPR arbetet. Så det är någonting som har påverkat utanför IT-avdelning så att säga. Vi har börjat samarbeta med den typen av frågor inom bolaget." (informant 1, 2018)*

På regional nivå arbetar ledningen på O1 med att införa nya regler och policys på löpande band istället för att ta allt i en och samma veva.

> *"Jag representerar ju ledning på [O1] Skåne så vi jobbar aktivt med att steg för steg införa nya regler och rutiner på hur det ska göras och hanteras. Jag försöker undvika att komma med en wall of text på tio sidor och säga "nu måste ni kunna GDPR" utan det är små portioner hela tiden istället." (Informant 1, 2018)*

4.1.2 Attityder vid organisationsförändring

Samtliga informanter har understrukit att attityden till det nya direktivet är varierande och skiljer sig mellan såväl anställda som ledning. Informant 1 och 2 beskriver att flera organisationer som de arbetar för inte tror att GDPR kommer att gälla dem. De berättar att de måste poängtera för deras kunder att GDPR är något som kommer påverka alla som hanterar personuppgifter.

> *"Det är mycket såhär blame game hos vissa kunder och att någon kund i kedjan anser att det här är deras leverantörs ansvar, vi friskriver oss från allting, ni måste ta hand om allting. Och det fungerar inte heller" (Informant 1, 2018)*

Informant 2 beskriver ett liknande attitydproblem:

> *"Det är många som försöker hitta en workaround. Exempelvis organisationer som gör automatiskt opt-in om du inte hör av dig. Det är fel. Du ska själv välja att göra en opt-in." (Informant 2, 2018)*

Informant 2 och 4 som är konsulter och har arbetat med ett antal kommuner menar på att attityden mellan den privata och offentliga även sektorn skiljer sig. De anser att offentlig sektor generellt är sämre förberedda för förordningen. Detta stärks av Informant 3 som arbetar inom offentlig sektor och menar på att detta påverkar attityden hos anställda inom organisationen. Informant 3 berättar:

> "*Det har börjat bli lite såhär: vi får väl vänta och se vad som händer. De kommer inte sätta dit oss, vi är ju offentlig sektor." (Informant 3, 2018)*

Genomgående har alla informanter tryckt på vikten av att utbilda sin personal inom området för att stärka attityden och förståelsen hos både kund och anställda. Det skiljer sig dock på utbildningens omfattning hos de olika organisationerna.

Informant 3, som sitter i projektgruppen för GDPR-arbetet har haft en mycket kort utbildning och menar på att hen förlitar sig på att det interna personuppgiftsombudet skall agera som stöttepelare vid frågor. För att involvera de som blir berörda av arbetet har de även haft workshops. Informant 1 menar att utbildningarna har skett på löpande band för att få alla så involverade som möjligt.

> *"Alla har fått en obligatorisk utbildning om en timme. Och vissa har fått det flera gånger. Dom i ledande ställning har fått lite utförligare utbildning."*
> *(Informant 1, 2018)*

En annan IT-konsult pratar om vikten att utbildning sker både internt och ute hos kund.

> *"Hos kund har de gjort så att vi har haft utbildningstillfällen och det har vi fortfarande. Stora organisationer så då har vi utbildningstillfällen hela tiden där de får svara på frågor. Vi har massa möten med dem för att vi ska kunna skapa den här ROPAN som det kallas, Record of Process activities."*
> *(Informant 2, 2018)*

4.2 Problematiken kring nya lagar och policys

Kunskapen om dataskyddsförordningen hos informanterna håller hög nivå eftersom de ansvarar för arbetet med GDPR både internt och externt. Trots detta har det under de intervjuer som har gjorts framkommit att majoriteten av informanterna trots bra kompetens inom området fört fram att tolkningen av lagen är en utmaning i den kommande dataskyddsförordningen. Informant 2 jobbar som projektledare och är ansvarig för GDPR-arbetet både internt och hos kund. Han menar att utmaningen ligger i att man får tolka lagen själv.

> *"Sättet du tolkar förordningen på är sättet du läser den på, så beroende på vilken människa du är och vilken nivå du ligger på så kommer du att läsa den på ett annorlunda sätt. Jag har alltid sagt att förordningen ska läsas för vad den är."*
> *(Informant 2, 2018)*

Informant 2 fortsätter:

> *"Den svåraste utmaningen har väl varit att man ska göra så pass mycket, men det finns liksom inget tillvägagångssätt med förordningen." (Informant 2, 2018)*

Något informanterna har gemensamt är att de med tiden av förändringsarbetet har insett att förordningen ställer större utmaningar på organisatoriska förändringar än tekniska aspekter.

> *"[...] Från den allra första början trodde jag att det skulle handla mer om tekniken än vad det gör, det handlar egentligen väldigt lite om teknik utan det handlar mer om mjuka processer […]" (Informant 1, 2018)*

Resterande informanter anser precis som informant 2 att det är problematiskt att lagen är tolkningsbar. Vidare menar olika informanter att tolkningsutrymmet och avsaknaden av rättspraxis i vissa fall resulterar i att de väljer att vänta och se hur det utspelar sig efter lagen är införd. Informant 3 som jobbar på en av Skånes största organisationer berättar att avsaknaden av rättspraxis gör att dem inte är helt säkra på vilken nivå de måste ligga på för att tillmötesgå förordningen**.**

> *"Vi får chansa lite och lägga en ribba. Sen får rättspraxis visa om vi måste göra en ny avvägning. Till exempel information till den registrerade, ja på vilken nivå, det vet vi inte riktigt än. (Informant 3, 2018)*

För att få en klarare bild av nivån informanterna måste lägga sig på, har organisationerna haft lite olika tillvägagångssätt. Det finns en del likheter mellan hur organisationerna tacklar problemet idag. Att bedriva ett samarbete mellan personer med olika kompetensområde är något som samtliga av respondenterna har tagit upp som väsentligt för att få en bredare översikt för förändringsarbetet. Informant 1 berättar:

> *"Vi har samarbetat med en advokatfirma där vi har utbildat dem inom de tekniska aspekterna och dom har utbildat oss inom de juridiska aspekterna inom GDPR. Som vi har haft ett fortlöpande samarbete med."*

Både informant 1 och 2 har deltagit i utbildningar hos datainspektionen. De menar att detta har gett dem en klarare bild över vad fokus bör ligga på. Respondenterna menar på att fokus från datainspektionens sida kommer att vara att kolla på hur organisationer arbetar och till vilken grad de försöker dokumentera och motivera varför och hur de behandlar personuppgifter snarare än att följa reglerna till hundra procent. Informant 1 berättar:

> *"När man läser lagen finns det mycket tolkningsutrymme men lyssnar man istället på vad datainspektionen säger så är dom väldigt tydliga med att det dom kommer fokusera på är vilka intentioner vi har haft." (Informant 1, 2018)*

> *"Ifall datainspektionen bedömer att vi har brutit mot GDPR så kommer dom titta mycket på hur mycket vi har försökt följa GDPR. Och mindre på detaljfrågorna, vad har vi faktiskt gjort för att följa GDPR." (Informant 1, 2018)*

4.3 Övriga utmaningar

4.3.1 Rutiner för efterlevnad

Informant 1, 2 och 4 påpekar att det finns kunder och andra organisationer som inte tar efterlevnadsaspekten på allvar. De menar att det finns en utmaning i att få företagen att förstå att arbetet måste fortgå efter den 25:e maj.

> *”Jag tror att gamla organisationer som inte förstår sig på detta kommer tro att datainspektionen ska glida in och börja inspektera bolaget, och om de inte gör det den dagen så är man lugn och så släpper man allt. Det är ett stort misstag om man gör det.” (Informant 2, 2018)*

Informanterna är tydliga med att poängtera att de internt jobbar för att säkerställa att arbetet med GDPR inte slutar den 25:e maj, men att det är en utmaning.

> *Utmaningen ligger i att förvalta det här över tid och där finns ju en osäkerhet just nu känner jag i hur mycket tid och ansträngning, energi kommer det att ta.” (Informant 1, 2018)*

Informant 1 fortsätter:

> *“När vi vet var vi kommer landa där, då kan vi analysera vad det kommer kräva i arbetsinsats att upprätthålla det här. Vi måste se till att alla nyanställda blir insatta till exempel, eller vi måste en gång om året om det har kommit några nya IT-system som vi inte känner till som vi måste inspektera eller vad det nu kan vara.”*

Informant 2 menar att de jobbar aktivt för att kunna efterleva den nya förordningen.

> *“Du ska ha en efterlevnadsplan, actions och to-do lists på vad du ska göra och hur du ska fortsätta arbeta med det, vilket alla organisationer måste ha.” (Informant 2, 2018)*

Som tidigare nämnt är respondenterna eniga om att den stora förändringen är på ett organisatoriskt plan snarare än tekniskt. Informant 3 säger att dokumentationen är en viktig del för att uppnå efterlevnad och för att vara redo den 25:e maj.

> *“Men väldigt mycket handlar om att dokumentera, hur vi tänkte. Så här tänkte vi, det kan vara fel men vi har iallafall tänkt, det är en jätteviktig del av processen.” (Informant 3, 2018)*

Som en del i att kontrollera om kunder efterlever förordningen den 25:e maj så kommer ett av konsultbolagen att utföra stickkontroller efter den 25:e maj.

> *“ […] Den 26:e maj kommer vi att börja med kontroller och stickprover för att se hur arbetet går. Det är bättre att vi gör det först än att datainspektionen kommer och knackar på dörren. Vi börjar därför med granskningsarbetet den 26:e maj redan för att se om allt ligger på plats.” (Informant 4, 2018)*

4.3.2 Otillräckliga avtal

På frågan om informanterna upplever några övriga utmaningar som GDPR-arbetet medför svarade tre av dem att det är problematiskt att rådande avtal angående personuppgiftshantering med leverantörer inte är tillräckliga i dagsläget för att tillmötesgå de krav på PuB-avtal som de anser att GDPR kräver.

> *"Många har underleverantörer utan bra pub-avtal. Många behöver instruktioner till sina pubavtal och ifall något händer och du ska bli frånlöst från allting. Processer, tillvägagångssätt hur ni hör av er till oss, hur vi hör av oss till er. De delarna måste komma på plats och allting som kommer på teknisk nivå." (Informant 2, 2018)*

Informant 3 och 4 belyser även att hanteringen av avtal är en stor utmaning. De menar att det är många avtal som måste revideras och att det är viktigt att relationerna skall fungera. Informant 3 berättar även att det finns problematik om man använder sig av någon annan leverantörs PuB-avtal eftersom någon då behöver sitta och granska det.

4.3.3 Redundant data & inventarier av system

Av respondenterna menar informant 2 och 4 att många av kunderna de arbetar hos har haft dålig koll på systemen och att det är svårt för dem att veta om de upprätthåller kraven. Två av de intervjuade personerna menar på att man har dålig koll på systemarkitekturen och var informationen lagras. På frågan om det fanns övriga utmaningar med GDPR-arbetet som vi inte hade behandlat svarade informant 3:

> *Ja, den här ostrukturerade massan som är ostrukturerade filer som man kunde strunta i innan. Där var vi lite, ska vi eller ska vi inte. Och då valde vi i höstas att vi kör på det också. Och det har inneburit hela det här städfokuset. Vi har inte varit bra på att gallra, alltså slänga grejer när vi ska […]. (Informant 3, 2018)*

Informant 1 delar informant 3s uppfattning om att det är utmanande att veta var data finns:

> *"Förr när man utvecklade mjukvaror och system och databaser och man slarvade med att man skulle kunna plocka bort data för att data ska alltid ligga kvar och det är en grej som jag tror att de flesta har en utmaning med." (Informant 2, 2018)*

> *"Man har inte vetat om arkitekturen man sätter ut i grunden på alla system. Men sen när man sätter sig och allvarligt ska ta fram det för att få en förståelse för hur informationen går så inser man ju nånstans att det här var mer komplext än vad vi tänkte oss." (Informant 2, 2018)*

Informant 1 menar att det ur ett tekniskt perspektiv har varit utmanande att kunder samlar in data till ändamål de inte känner till och att detta har resulterat i att det är svårt att veta var data ligger lagrad. Informant 2 belyser samma problem:

> *"Det har visat sig många gånger att det finns redundant information, så om du plockar bort något så finns det kvar i systemet ändå." (Informant 2, 2018)*

Samtliga informanter berättar att inventarier av systemen pågår eller har genomförts men att det är en komplex process som kräver mycket resurser och tar lång tid. Informant 3 menar att IT-inventeringen har skett parallellt med åtgärdsplaneringen.

> *"Vi känner till 850 system som vi har inventerat 400 av, men alla innehåller inte personuppgifter. Dom flesta prioriterade system är inventerade utifrån ett frågeformulär. Det betyder inte att vi har åtgärderna på plats."* (Informant 3, 2018)

5 Diskussion

Utifrån empirin kan vi urskilja ett antal utmaningar som organisationerna finner problematiska och hur de intervjuade informanterna hanterar dem. För att vidare hålla den röda tråden har vi valt att utgå från de rubriker som sammanställdes i den teoretiska översiktstabellen. I diskussions och analysdelen syftar vi till att presentera likheter, skillnader och andra intressanta aspekter som kan kopplas till teorin.

5.1 Utmaningar & förändringsarbete

Precis som Burnes (2009) skriver är det vid förändring viktigt att företagen identifierar hur de bedriver sin nuvarande verksamhet och hur de vill se ut i framtiden, vilket även inkluderar förändringsarbetet med GDPR. Uppfattningen är att samtliga informanterna har arbetat aktivt med att försöka förhålla sig till förordningen men att de fortfarande står inför ett antal utmaningar. Enligt informanterna var den generella uppfattningen tidigt i förändringsarbetet att fokus låg på de tekniska utmaningarna men att de i slutskedet av arbetet har kommit till insikt att de största förändringarna har och är tvungna att ske på en organisationsnivå. Vidare menar informanterna att många av deras medarbetare och kunder har olika attityder kring omfattningen som det nya dataskyddsdirektivet medför.

5.2 Organisationsförändring

5.2.1 Ledning vid organisationsförändring

Kotter (1995) och Smith (2005) betonar hur viktigt det är för ledningsgruppen inom en organisation att skapa en tydlig vision om varför förändringen är nödvändig för verksamheten och konstant kommunicera den inom organisationen. Överlag har informanterna beskrivit att ledningen har spelat en stor roll för att förankra förändringsarbetet mot GDPR inom organisationerna, dock i olika omfattning.

Tre av fyra av informanterna jobbar som konsulter på It-bolag som har god kompetens inom datasäkerhet och informationshantering, där ledningen arbetar aktivt för att förankra arbetet inom organisationerna. Detta tror vi bidrar till att de överlag har en ledning som generellt förstår allvaret med förordningen bättre än andra branscher. Kotter (1995) förklarar vidare att det är viktigt att man tar bort de hinder som är i vägen för förändring. Två av informanterna har beskrivit att det har varit problematiskt i den mån att varje regionalt kontor tidigare har varit isolerade öar i bemärkelsen att de har haft olika arbetsmetoder och policys. De menar att arbetet med GDPR har tvingat organisationerna att samarbeta mellan olika regionkontor för att utveckla policys och riktlinjer på koncernnivå och att detta är något som har fört dem närmare.

Fastän vissa av informanterna anser att ledningen internt arbetar hårt för att förankra GDPR-arbetet belyser de problematiken kring bristande kunskap och förståelse från ledningen ute hos kund. Denna problematik framgår tydligt i organisationen där informant 3 arbetar. Vi

tolkar det som att ledningen på O3 inte har tagit arbetet med GDPR på lika stort allvar som resterande informanternas organisationer. Informant 3 beskriver att arbetet med GDPR har varit problematiskt i den mån att projektet har haft problem att nå upp i organisationen eftersom ledningen inte har kompetensen eller förmågan att se allvaret i förändringsarbetet. Moran och Brightman (2000) belyser vikten av att ledningen skall förstå betydelsen av förändringen och hur de skall arbeta för att uppnå ett lyckat förändringsresultat, något som verkar vara bristande i verksamheten där informant 3 arbetar. I enlighet med Chapman (2002) är det även viktigt att ledningen vet vilka resurser som behöver avsättas, vilket är något som informant 3 menar är problematiskt i den mån att hen hade önskat att fler personer är involverade i projektet.

5.2.2 Attityder vid organisationsförändring

Kotter (1995) menar att tydliga visioner kan hjälpa till att skapa förståelse för varför specifika verksamhetsprocesser behöver förändras. För att kunna applicera och efterleva det nya direktivet krävs det att man förändrar såväl beteenden som attityder hos anställda. Samtliga informanter menar att attityderna kring det nya direktivet är väldigt olika, vilket kan vara ett resultat av att uppfattningen och kunskapen om förordningen ser olika ut från organisation till organisation.

En av informanterna pratar om de olika attitydnivåerna och menar på att många ligger på en låg-medelnivå. Två andra informanter upplever även att det är en utmaning att få företagen de arbetar med att inse att de kommer att påverkas av den kommande förordningen. Exempel på detta är informant 1 uttalande om att det är många i kedjan som försöker frånskriva sig ansvaret på systemleverantörerna och att det är deras uppgift att kraven enligt GDPR uppfylls. För att få hela organisationen att förstå hur och varför förändringen ska ske krävs det att personalen är väl införstådda (Armenakis et al., 1993). Kotter (1995) och Mendoza et al. (2016) menar att detta kan underlättas genom att utbilda personal och sammanställa tydliga riktlinjer och policys. Utbildning av personal är något som alla informanter har genomfört internt för att skapa en större förståelse för vad förordningen kommer att innebära, något som även Puhakainen & Siponen (2010) menar är viktigt. Två av informanterna som har intervjuats har även haft många utbildningstillfällen ute hos kund, för att besvara de frågor som det råder oklarheter kring. Samtidigt menar informant 3 att det är problematiskt att projektgruppen förväntas kunna svara på frågor som kommer från anställda, men att de själva har svårigheter att förstå vissa delar och därför inte kan besvara alla frågor. Om anställda inte får ta del av den information som de efterfrågar kan det bidra till försämring av attityd till förändringen. Detta står i kontrast till Jones et al. (2005) teori om att anställda som får ta del av högkvalitativ information kommer att vara mer tillmötesgående.

Även om arbetet med GDPR är utmanande menar informant 1 att GDPR är positivt i bemärkelsen att förordningen tvingar dem att förbättra de verksamhetsprocesser som hanterar personuppgifter, vilken hen anser att de borde ha gjort för länge sedan. På samma sätt menar Kotter (1995) att det är viktigt att identifiera både potentiella hot men även möjligheter som en förändring medför. Vi tror att verksamheterna kan dra nytta av att försöka se möjligheterna och inte bara nackdelarna med GDPR-arbetet. På så sätt kommer det att bli lättare för dem att förankra förordningen och uppnå efterlevnad inom respektive organisation.

En intressant aspekt som vi inte ämnat undersöka men som framkommit är att attityden mellan organisationer inom offentlig och privat sektor skiljer sig markant enligt våra

informanter. Informanterna anser att den offentliga sektorn generellt är sämre förberedda än den privata. Detta kan bero på att attityden för förändring och kompetensen inom den offentliga sektorn är sämre. Detta stärks av informants 3 uttalande:

> *"De kommer inte sätta dit oss, vi är ju offentlig sektor."*

5.3 Problematiken med nya lagar och policys

Massey, Otto, Hayward & Anton (2009) beskriver lagtolkning som ett vanligt förekommande problem när nya regelverk sätts i bruk. Detta är något som alla informanter menar har varit problematiskt, dock i olika utsträckning. Det är framförallt två av informant som menar att problematiken kring lagens tolkningsutrymme har gjort att det är svårt att fastställa vilken nivå man bör ligga på för att tillmötesgå kraven till den 25:e maj. De menar att det inte finns några specifika tillvägagångssätt för verksamheterna att följa för att leva upp till förordningen, vilket resulterar i att de vet hur lagen lyder, men inte exakt hur arbetet ska genomföras. Precis som Otto och Anton (2007) beskriver är dataskyddslagar och lagar inom informationssäkerhet relativt nya vilket vi tror kan vara en anledning till att respondenterna har svårt att veta hur de ska förhålla sig till lagen.

Mendoza et al. (2016) menar att det är lättare att efterleva en förordning om det finns handböcker eller tidigare prejudikat att gå efter. Informanterna har betonat att de har svårt att veta hur mycket resurser som skall tillsättas och på vilken nivå de måste ligga på för att uppfylla kraven. Det som kan utläsas från empirin är att informant 1 och 3 har valt att lägga sig på en nivå och sedan avvakta en del av arbetet tills de vet hur datainspektionen kommer att agera och tills det finns rättspraxis att gå efter. Detta är ett exempel på hur lagens tolkningsutrymme resulterar i olika tillvägagångssätt. Det som även kan utläsas är att de informanter som har varit på utbildning hos datainspektionen generellt verkar ha fått en klarare bild över vad som behöver göras innan den 25:e maj, till skillnad från resterande informanter. De menar på att datainspektionen kommer att lägga stor vikt på att titta på vilka intentioner de har haft. Detta inkluderar motiveringar till personuppgiftslagring och hur länge de lagras, snarare än att på detaljnivå kolla om varje aspekt av förordningen följs. De menar att de även har fått större förståelse av att delta i diskussioner med andra företag på plats. Majoriteten av informanterna berättar att de arbetar tillsammans med externa jurister för att få en djupare förståelse för förordningen och hur den skall tolkas, något som även Mendoza et al. (2016) menar kan vara av nytta för en organisation vid tolkning av nya lagar.

5.4 Övriga utmaningar

5.4.1 Rutiner för efterlevnad

Informanterna menar att GDPR är ett fortlöpande arbete som kommer att behöva ses över på lång sikt. Tre av informanterna menar att det på grund av olikheter i attityder blir problematiskt att skapa förståelse hos de som tror att förordningen kommer att falla mellan stolarna. Det råder dessutom osäkerhet i hur man skall förankra förordningen över tid samt hur mycket ansträngning och resurser som kommer krävas. Detta kan även vara ett resultat av

att man inte vet hur man skall gå tillväga. Sannolikt är det även därför majoriteten av informanterna har valt att vänta och se tills rättspraxis får avgöra om de har tillsatt tillräckligt med resurser. Därför fokuserar flera av informanterna på att utveckla åtgärdsplaner som skall fungera efter den 25:e maj.

En stor del av förarbetet har grundat sig i att försöka kartlägga och dokumentera hur organisationerna bedriver sin nuvarande verksamhet, vilket enligt Burnes (2009) är viktigt om man på ett framgångsrikt sätt vill nå det framtida tillståndet. Därefter berättar informanterna att sårbarhetsanalyser och kravanalyser har genomförts för att identifiera de processer som i nuläget inte lever upp till de krav som förordningen ställer. Detta återgår till Kotters (1995) teori om att det är viktigt att ta bort de hinder som är inte ligger i linje med visionen för att ta fram strategier om hur man bör gå vidare. Utifrån kravanalyserna och sårbarhetsanalyser har det utvecklats nya arbetsmetoder och riktlinjer. Att få samtlig personal till att följa dessa nya riktlinjer anser majoriteten av informanterna vara en utmaning.

5.4.2 Otillräckliga avtal

Fastän respondenterna är eniga om att organisatoriska aspekter är en viktig del för att efterfölja förordningen finns det en del tekniska och praktiska utmaningar som de står inför. Tre av informanterna tog upp problematiken med personuppgiftsbiträdesavtal vid en öppen fråga om övriga utmaningar.

Majoriteten av informanterna beskrev att hanteringen av PuB-avtal är en utmaning som kommer kräva mycket resurser och tid, bland annat måste man skriva om vissa avtal som finns mellan samarbetspartners. De menar att avtalen måste granskas och revideras så att de uppfyller de nya kraven som förordningen medför. Vi tror att detta är något som kan bli svårt eftersom det krävs en korrekt tolkning av lagen om alla delar av avtalen skall leva upp till förordningen. För att försöka tillmötesgå lagen på ett korrekt sätt menar en av informanterna att organisationen har tagit fram mallar som de menar ska hjälpa till att undvika eventuella problem. Detta är viktigt eftersom PuB-avtalen beskriver vem som är ansvarig vid ett eventuellt dataintrång (Datainspektionen, 2018g). Om det råder viss osäkerhet i vem som är ansvarig i avtalen finns det risk att organisationen bötfälls av anledningar som kan undvikas.

5.4.3 Redundant data & inventarier av system

GDPR ställer ökade krav på bland annat spårbarhet och transparens. Detta ställer tydligare krav på organisationer att de måste ha tydligare dokumentation om var, varför och hur data lagras och behandlas. Två av informanterna upplever att det är svårt att veta var data ligger lagrad och att det på flera ställen finns redundant information. Om en person begär att få ta bort sin data enligt borttagningsregeln ser vi en problematik om företagen inte kan säkerställa att datan även finns lagrad på andra platser. Detta kan leda till att organisationerna omedvetet bryter mot lagen och riskerar att bli bötfällda. För att lösa problemet menar två av informanterna att de kartlägger IT-infrastrukturen för att se var personuppgifter berörs. Även inventarier av aktuella system görs för att sålla bort den data som är överflödig.

6 Slutsats

I detta kapitel kommer fynden som gjorts och resultatet av uppsatsen att redovisas. Dessa fynd är baserade på empirin och den tidigare forskning som gjorts inom området. Kapitlet har som syfte att ge svar på forskningsfrågan som ställdes i kapitel ett. I slutsatsen presenteras vilka organisatoriska utmaningar som GDPR-ansvariga anser är problematiska vid förändringsarbetet mot den nya dataskyddsförordningen samt hur de går tillväga för att lösa dessa.

Vilka organisatoriska utmaningar anser GDPR-ansvariga är problematiska med förändringsarbetet inför den nya dataskyddsförordningen och hur går de tillväga för att lösa dessa utmaningar?

Teorin som har lyfts fram visar på vilka framgångsfaktorer som leder till ett effektivt förändringsarbete och varför det kan vara problematiskt att efterleva nya lagar och förordningar. Undersökningen gjordes i form av fyra kvalitativa intervjuer och har sedan ställts emot teorin för att skapa förståelse för de utmaningar som GDPR-ansvariga anser är problematiska.

Fastän dataskyddsförordning snart träder i kraft visar vår studie att det finns ett antal organisatoriska utmaningar som står i vägen för en del verksamheter. Det är påtagligt att informanterna är överens om att utmaningarna främst ligger i att genomföra förändringar på organisationsnivå, snarare än att utföra tekniska förändringar på detaljnivå. Avsaknaden av rättspraxis och utmaningen i att försöka tolka lagen har lett till att organisationer tvingats göra egna bedömningar angående reglerna i förordningen. Detta har i vissa fall lett till att organisationer valt att lägga sig på en nivå och sedan avvakta rättspraxis för att se om det behöver göras justeringar.

Undersökningen visar även att det finns bristande kunskaper om förordningen vilket manifesterar sig genom att en del organisationer inte är medvetna om på vilka sätt förordningen kommer att påverka dem. Vidare påvisar undersökningen att det är problematiskt att förankra de nya riktlinjer och rutiner som har skapats för att möta de nya kraven. Det råder också en osäkerhet över hur mycket resurser det kommer att krävas att förvalta arbetet över tid.

Att ledningen är en viktig faktor vid organisationsförändring är något som tydligt framgår av teorin och informanterna. Trots detta visar undersökningen att en del GDPR-projekt har svårt att få ledningen att förstå allvaret och omfånget av förändringsarbetet. Detta i sin tur försvårar arbetet med att förankra förändringarna i organisationer, vilket kan vara ett resultat av att de tolkar den på olika sätt. De organisationer som har undersökts har hanterat utmaningarna på olika sätt, men något som är gemensamt är vikten av att skapa förståelse i form av utbildning och att ledningen aktivt är med och förankrar arbetet inom organisationen.

7 Förslag på vidare forskning

Denna studie är genomförd innan den nya förordningen sätts i bruk. Det kan därför vara av intresse att genomföra en liknande studie efter förordningen har börjat gälla, för att undersöka om liknande problemen kvarstår och om organisationernas tillvägagångssätt har varit effektiva. Undersökningen har inte fokuserat på en specifik bransch men det kan vara intressant att undersöka utmaningar som är branschspecifika. Något som har indikerats men som inte har varit av relevans för denna undersökning är skillnaden mellan privat och offentlig sektor. Vi ser ett intresse av att kolla på varför den privata sektorn generellt anses vara bättre förberedd än den offentliga sektorn.

8 Referenser

Achilles A. Armenakis, Stanley G. Harris, and Kevin W. Mossholder (1993). Creating Readiness for Organizational Change. *Human Relations*. Vol 46, Issue 6, pp. 681 - 703

Anderson, D., & Anderson, L. A. (2002). *Beyond Change Management: Advanced Strategies for Today's Transformational Leaders*. John Wiley & Sons.

Baker & McKenzie (2016*). Preparing for new privacy regimes: Privacy professionals' views iews on the general data protection regulation and privacy shield*.

Brook, D. (2018). GDPR puts vendor contracts in the security spotlight. *Computer Fraud & Security,* Vol 2018, Issue 4, pp. 5-7

Burnes, B. (2009). *Managing Change: A Strategic Approach to Organisational Dynamics*. Pearson Education.

Chapman, J. A. (2002). A framework for transformational change in organisations. *Leadership & Organization Development Journal*, 23(1), 16–25.

Datainspektionen. (2018a). Personuppgiftslagen.
https://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/
[2018-04-12]

Datainspektionen (2018b). Introduktion till dataskyddsförordningen.
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/introduktion-till-dataskyddsforordningen/
[2018-04-12]

Datainspektionen (2018c) Strukturerat eller ostrukturerat.
https://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/strukturerat-eller-ostrukturerat/
[2018-04-14]

Datainspektionen (2018d). Vad är en personuppgift.
https://www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/vad-ar-en-personuppgift/
[2018-04-17]

Datainspektionen (2018e) Skyldigheter för de som behandlar personuppgifter.
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/skyldigheter-for-de-som-behandlar-personuppgifter/personuppgiftsansvarig/
[2018-04-25]

Datainspektionen (2018f) Personuppgiftsbiträde.
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/skyldigheter-for-de-som-behandlar-personuppgifter/personuppgiftsbitrade-och-bitradesavtal/
[2018-04-25]

Datainspektionen (2018g) Personuppgiftsansvar och personuppgiftsbiträden. https://www.datainspektionen.se/fragor-och-svar/eus-dataskyddsreform/personuppgiftsansvar-och-personuppgiftsbitraden/?id=2585#avtal [2018-14-25]

Datainspektionen (2018h) Rätt till information. https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registrerades-rattigheter/ratt-till-information/ [2018-04-24]

Datainspektionen(2018i) Register över behandling. https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/skyldigheter-for-de-som-behandlar-personuppgifter/register-over-behandling/ [2018-04-24]

Datainspektionen (2018j) Rätt till rättelse. https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registrerades-rattigheter/ratt-till-rattelse/ [2018-04-24]

Datainspektionen (2018k) Rätt till radering. https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registrerades-rattigheter/ratt-till-radering/ [2018-04-24]

Datainspektionen (2018l) Dataportabilitet. https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registrerades-rattigheter/dataportabilitet/ [2018-04-24]

Davenport, T. H., & Prusak, L. (2000). Working Knowledge: How Organizations Manage What They Know. *Harvard Business Press*.

Eu.Riksdagen (2018). Olika typer av EU-lagar. https://eu.riksdagen.se/vad-gor-eu/en-eu-lag-blir-till/eus-lagar-och-regler/# [2018-04-25]

Gilley, A., McMillan, H. S., & Gilley, J. W. (2009). Organizational Change and Characteristics of Leadership Effectiveness. *Journal of Leadership & Organizational Studies*

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research*, 59(6), 703–705.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. *Decision Sciences*, 43(4), 615–660.

IBM. (2018). Data management: Tapping your most valuable asset. https://www.ibm.com/midmarket/us/en/article_DataManagement2_1209.html [2018-05-09]

Jacobsen, D (2002). *Vad, Hur Och Varför?: Om Metodval I Företagsekonomi Och Andra Samhällsvetenskapliga Ämnen.* Lund: Studentlitteratur.

Jones, R. A., Jimmieson, N. L., & Griffiths, A. (2005). The Impact of Organizational Culture and Reshaping Capabilities on Change Implementation Success: The Mediating Role of Readiness for Change. *Journal of Management Studies*, 42(2), 361–386.

Kotter, J. (1995). Leading change: Why transformation efforts fail. Boston: *Harvard Business School Press.*

Massey, A. K., Otto, P. N., Hayward, L. J., & Antón, A. I. (2009). Evaluating existing security and privacy requirements for legal compliance. Requirements Engineering, 15(1), 119–137.

Mendoza, J. P., Dekker, H. C., & Wielhouwer, J. L. (2016). Firms' compliance with complex regulations. *Law and Human Behavior*, 40(6), 721–733.

Moran, J. W., & Brightman, B. K. (2000). Leading organizational change. *Journal of Workplace Learning*, 12(2), 66–74.

Otto, P. N., & Anton, A. I. (2007). Addressing Legal Requirements in Requirements Engineering. In *15th IEEE International Requirements Engineering Conference* (RE 2007)

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, 34(4), 757-778. doi:10.2307/25750704

Rune Todnem By. (2005). Organisational Change Management: A Critical Review. In The Principles and Practice of Change (pp. 46–58).

Salon, O & Laughland, O. (2018, 2 maj). Cambridge Analytica closing after Facebook data harvesting scandal. *The Guardian.* Hämtad från https://www.theguardian.com/uk-news/2018/may/02/cambridge-analytica-closing-down-after-facebook-row-reports-say [2018-05-15]

Schneider, B., Brief, A. P., & Guzzo, R. A. (1996). Creating a climate and culture for sustainable organizational change. *Organizational Dynamics*, 24(4), 7–19.

Smith, I. (2005). Achieving readiness for organisational change. *Library Managemen*t, 26(6/7), 408–412.

Weiner, B. J. (2009). A theory of organizational readiness for change. *Implementation Science:* IS, 4.

9 Bilagor

9.1 Intervjuguide

Inledande frågor:
1. Inom vilket arbetsområde är du verksam just nu och sedan hur länge?
2. När började ni/du arbeta med GDPR?
3. Har du genomgått någon form av utbildning om Dataskyddsförordningen?

Kategorier för frågor
Attityder vid organisationsförändring
4. I och med att det ännu inte har blivit implementerat är lagen fortfarande tolkningsbar. Har det funnits några svårigheter att tolka lagen?
5. I vilken mån utbildas personal inför GDPR?
6. Hur är attityden hos anställda kring direktivet (GDPR) idag?

Ledning
7. Arbetar ledningen aktivt med att förmedla hur man skall arbeta med den nya lagen?
   - Om ja, hur engageras medarbetare i arbetet med GDPR?

8. När det gäller attityder hos anställda, vilken är den svåraste utmaningen?

Organisationsförändring
9. Har ni upplevt att arbetet med GDPR påverkat företaget på ett sätt ni inte förväntat er?
   - Om ja, på vilket sätt?
10. Har arbetet med GDPR kostat mer än vad ni hade tänkt er rent monetärt?
11. Vilka utmaningar för själva organisationen tycker du att arbetet med GDPR har medfört?
   - Kan du motivera detta lite närmare?
12. Finns det fler utmaningar utöver de som vi har diskuterat som ni står inför?
   - Varför är det en utmaning?
   - Har ni upplevt några problem redan nu med dessa utmaningar?

Regler
13. Måste din organisation genomföra omfattande förändringar i sina IT-system för att kunna efterleva Dataskyddsförordningen?
   - Om ja, på vilket sätt?
14. Måste ni avsätta nya resurser för att kontrollera att lagarna följs?
15. Den nya lagen kräver att man ordnar upp i ostrukturerade data. Har ni idag uppgifter i ostrukturerade data?
   - Hur stort problem är detta?

9.2 Intervjuer

9.2.1 Intervju 1 – Informant 1

Intervjuare - Jens Andersson (JA)
Sekreterare - Edward von Essen
Informant 1 - Teknikchef på O2 region syd avdelning. Arbetat med datasäkerhet i över 5 år och med GDPR i 1.5 år.

START

1 JA: Inom vilket arbetsområde är du verksam just nu och hur länge?

2 Informant: Min roll är director of technology på (O1) skåne, vilket i princip är CTO eller teknikchef eller något åt det hållet, vilket innebär att jag har ett övergripande ansvar över att hålla koll på vilka kompetenser vi har inom företaget. Och att vi kan rätt saker, vi utbildar oss och vem som är bäst lämpad att göra saker. Som ett sidospår till det har GDPR smugit sig in. Det är nog mest mitt egna fel men det senaste året, ett och ett halvt år har jag utbildat många av våra kunder och även internt på företaget. Så egentligen är jag inte ansvarig att arbeta med GDPR men det har fallit på min stol att göra det. I den rollen jag har nu har jag suttit sen i somras. Men jag ha jobbat med GDPR lång tid innan dess, i form av arkitektur eller ja jag har utbildat inom GDPR långt innan dess.

3 JA: Jag undrar, har du jobbat internt med GDPR inom ditt företag också?

4 Informant 1: Ja. Jag tror bakgrunden till det är att innan i somras var jag i en roll som arbetade direkt till kunder som vilken konsult som helst, men sen i somras har jag jobbat internt och som en rådgivande kapacitet till våra kunder. Jag har aldrig några heltidskonsult uppdrag längre utan det är mer en timme här och där ute hos kunder. Så där har jag fortfarande kvar mycket kundkontakt och framförallt inom GDPR frågor. Så där har jag kvar mycket kundkontakt. Jag håller i både utbildning internt och även genomförande internt. Både på lokal skallnivå men även för (O1) international. Det är mycket GDPR nu.

5 JA: Nu har du redan besvarat vår andra och tredje fråga som var, när började du arbeta med GDPR och vilken form av utbildning har du inom GDPR.

6 Informant 1: Alltså utbildning inom det har jag haft, från början var det bara att läsa skiten. Läsa alla dokument som fanns tillgängliga. Jag har även varit på två utbildningar hos datainspektionen. Vi har samarbetat med en advokatfirma där vi har utbildat dem inom dom tekniska aspekterna och dom har utbildat oss inom dom juridiska aspekterna inom GDPR. Som vi har haft ett fortlöpande samarbeta med.

7 JA: I och med att GDPR inte har blivit implementerat så är lagen fortfarande tolkningsbar. Det finns inga prejudikat att gå efter. Har det funnits några svårigheter att tolka lagen?

8 Informant 1: Alltså svårigheter, ja absolut det finns ju alltid en viss osäkerhet men framförallt, dom tveksamheterna som finns känns inte som dom spelar jättestor roll, alltså det är mycket, när man läser lagen finns det mycket tolkningsutrymme men lyssnar man istället på vad datainspektionen säger så är dom väldigt tydliga med att det dom kommer fokusera på är vilka intentioner vi har haft. När man lägger på den aspekten blir det, ja datainspektionen

kanske inte håller med oss att det här var exakt rätt att göra men om dom bara ser att vi har gjort förarbetet. Där vi har dokumenterat, så här har vi resonerat och därför har vi tagit det beslutet att betrakta det här som en personuppgift eller känslig personuppgift eller vad det nu kan vara. Då kommer dom acceptera det på ett helt annat sätt så därför, ja det är svårt att göra avgränsningar vad lagen kommer innebära exakt utan prejudikat men det är inte någonting som vi betraktar som en stor affärsrisk.

9 JA: Lagen finns ju den ser man, det här kommer att hända. Men har datainspektionen gett instruktioner på hur det ska göras?

10 Informant 1: Nej det har dom ju inte, utan mycket av instruktioner säger att ni måste tänka på, ni måste tänka på den här saken eller va de nu kan vara. Men däremot finns det instruktioner från datainspektionen som säger att, när datainspektionen bedriver sin tillsyn mot oss ska dom resonera på det här sättet. Ifall datainspektionen bedömer att vi har brutit mot GDPR så kommer dom titta mycket på hur mycket vi har försökt följa GDPR. Och mindre på hur detaljfrågorna, hur har vi faktiskt gjort för att följa GDPR. Eller det finns ett väldigt stort utrymme för datainspektionen att acceptera vårt arbete runt GDPR så länge vi inte har försökt komma undan GDPR på något sätt.

11 JA: Personal som inte är involverad i ert GDPR arbete, hur mycket information och utbildning har dom fått?

12 Informant 1: Alla har fått en obligatorisk utbildning om en timme. Och vissa har fått det flera gånger. Dom i ledande ställning har fått lite utförligare utbildning.

13 JA: Gäller det både internt och ute hos dina kunder eller är det bara internt på ditt företag?

14 Informant 1: Alla som är anställda av (O1) oavsett arbetsområde har fått utbildning ja. Även alla nyanställda får denna utbildning. Men det är inte så stort arbete att ge den utbildningen. Alla har det och sen så har vi då när det kommer till administrativ personal men den är inte lika omfattande beroende på vilket arbetsområde. Där sitter vi och kolla mer på vilka områden som kommer beröra dom endast.

15 JA: Hur är attityden hos anställda?

16 Informant 1: Väldigt varierande, oftast så spontant hos många mindre beredda kunder är ju att, äsch det här spelar ju ingen roll vi hanterar inte persondata, vi säljer ju däck eller vad det nu kan vara. Men då får man påpeka för dom att ni har ju kunder och anställda om inte annat så har ni åtminstone det. Det är väl en typ av attityd, en annan attityd oftast hos större bolag så är det att det sitter en riktigt administrativ jurist någonstans som ska lusläsa alla avtal och allting ska vara mycket finstilt och paragrafer hit och dit och då får vi hantera det. Det är mycket så här *blame game* hos vissa kunder och att någon kund i kedjan anser att det här är deras leverantörs ansvar, vi friskriver oss från allting, ni måste ta hand om allting. Och det fungerar inte heller, det är inte så GDPR fungerar vilket är väldigt bra. Det finns alla möjliga attityder.

17 JA: Arbetar ledningen aktivt med hur man ska arbeta med dom nya reglerna?

18 Informant 1: Ja det gör vi. Sen så beror det också på hur man ser på ledning. Jag representerar ju ledning på (O1) Skåne så vi jobbar aktivt med att steg för steg införa nya regler och rutiner på hur det ska göras och hanteras. Jag försöker undvika att komma med en

wall of text på tio sidor och säga ”*nu måste ni kunna GDPR*” utan det är små portioner hela tiden istället. Även att säga ”*från och med nu måste ni kryptera era hårddiskar på era datorer, från och med nu måste ni samla all data på ett komplett ställer”*. Men även från koncernens sida finns det direktiv högt uppe ifrån. Och det är på ett övergripande plan som trycks ner på mig då. Så här ska kunddata hanteras på (O1).

19 JA: Om vi tittar på andra företag som du arbetar med, är det någon skillnad på hur företag arbetar beroende på deras storlek? Har större företag en mer tydlig policy på hur man ska hantera detta?

20 Informant 1: Större företag har generellt mer policys överlag. Sen betyder inte den för sakens skull att dom bryr sig mer, utan det är mer att man har kapaciteten och man känner sig tvungen att ta fram en policy. Det ska finnas en policy för GDPR annars finns det inget sätt för dom att hantera det. Medan mindre företag egentligen bättre koll på GDPR men dom har inga policys. Jag tror det är mer att förhållningssättet hos de enskilda kunder som spelar roll och hur viktigt dom tycker GDPR är.

21 JA: har ni upplevt att arbetet med GDPR påverkat företaget på ett sätt ni inte förväntat er?

22 Informant 1: Nä, inte så väsentligt i alla fall. Det är klart att min förståelse för GDPR ökat allt eftersom, men det är klart att från den andra första början trodde jag att det skulle handla mer om tekniken än vad det gör, det handlar egentligen väldigt lite om teknik utan det handlar mer om mjuka processer, vad har vi?, hur säkerställer vi att vi har en rutin för det här? Vet vi vad vi gör och varför vi gör det? Den biten har blivit mer viktigt jämfört med den första blicken vi hade på GDPR.

23 JA: Har det varit problematiskt?

24 Informant 1: Det har varit problematiskt på det sätt, att det hade varit jätte enkelt om det bara hade varit tekniska aspekter. Då krypterar vi bara alla hårddiskar så skulle det vara klart. Det kan vi även mäta och checka av i en checklista. Men att säkerställa att organisationen följer rutiner är mycket svårare. Det är svårare att följa rutiner än att ta fram krav på hur vi utvecklar framtida applikationer och så är vi färdiga.

25 JA: Har det kostat mer än vad ni tänkt er rent monetärt?

26 Informant 1: Ja det har det absolut. Så fort vi börjar jobba med mjuka processer blir det dyrare. Hade vi bara behövt ändra i våra system så hade man gjort det och så hade det varit färdigt. Nu är det mer återkommande i den bemärkelsen att vi är aldrig kommer vara färdiga med det här arbetet. GDPR kommer aldrig vara färdigt utan det kommer fortsätta att verka och det kommer förändra hur vi arbetar. På i grund och botten ett väldigt bra sätt, men det är klart att det är en kostnad.

27 JA: Vilka utmaningar för organisationen i sin helhet och inte bara IT-avdelningen har GDPR medfört?

28 Informant 1: I mitt perspektiv så, vi har varit väldigt decentraliserade och är fortfarande ett decentraliserat bolag i den bemärkelsen att (O1) Skåne är relativt fristående från (O1) Göteborg och alla andra. Vi är väldigt isolerade öar när det kommer till IT och centrala policys och den typen av saker. Men i och med att det här slår på en koncern nivå så måste koncernen ta ett helhetsgrepp på väldigt stora bitar av GDPR arbetet. Så det är någonting som

har påverkat utanför IT-avdelning så att säga. Vi har börjat samarbeta med den typen av frågor inom bolaget. Så det tar oss tillbaka till förra frågan. Det är väldigt lite teknik och mer människor och processer i det här. Vi har ingen dedikerad IT-avdelning på det sättet här. På så sätt har det framförallt påverkat andra bitar än IT-avdelningen. Exempel hur vi skriver våra kundavtal och hur vi skriver våra anställningsavtal och så vidare.

29 JA: Är det någon utmaning som du känner att vi inte har tagit upp?

30 Informant 1: Asså den stora utmaningen som jag ser på det här, är att få det här att leva vidare och få organisationer att betrakta det här inte som ett projekt utan någonting som ska leva kvar. Utmaningen ligger i att förvalta det här över tid. Och där finns ju en osäkerhet just nu känner jag i hur mycket tid och ansträngning, energi kommer det att ta. Det vet vi inte riktigt förrän vi vet var vi landar. Just nu formar vi fortfarande var vi kommer landa 25 maj. När vi vet var vi kommer landa där, då kan vi analysera vad det kommer kräva i arbetsinsats att upprätthålla det här. Vi måste se till att alla nyanställda blir insatta till exempel, eller vi måste en gång om året om det har kommit några nya IT-system som vi inte känner till som vi måste inspektera eller vad det nu kan vara. Någonting åt det hållet kommer att behövas i alla fall. Och det ser jag som det stora långsiktiga problemet.

31 JA: Det för oss in på nästa fråga. Du sa att det inte kommer påverka tekniken så mycket, i alla fall inte så mycket som ni har trott. Är det så här eller hos kund att dom kommer behöva göra omfattande ändringar i befintliga system? Och i så fall på vilket sätt?

32 Informant 1: Dom flesta behöver inte göra jättestora förändringar, därför att nästa alla våra kunder och nästan all typ av behandling vi utför, utförs inom ramen av ett avtal. Om vi tänker till exempel att vi har en kund som bedriver e-handel så måste dina personuppgifter behandlas i webbshopen, i deras bokföringssystem och leveranssystem och andra system. Allt det går att täcka, det är rätt lätt att få det att fungera med GDPR. Den stora biten har egentligen varit att föröka att arbeta med Big Data, att dom samlar in data till ändamål som dom inte känner till. Men det är ett rent organisatoriskt problem. Det är mer en form av hur dom använder data. Ur ett tekniskt perspektiv har dom stora utmaningarna legat i kunder som jobbat mycket gränser och det kanske är svårt att veta var data finns.

33 JA: Det måste ändå ha gjorts ganska omfattande inventarier av data? Särskilt större företag har data på väldigt många olika ställen.

34 Informant 1: Exakt, det är bara att kolla här på (O1), dom excelbladen och ställen vi har data på, som vi nu rationaliserar ner och skalar bort. Mest för att vi ska slippa mer administration. Vi behöver egentligen inte ändra någonting för GDPR utan det är mer att rent egenintresse försöker vi minska antalet plaster och sätt att behandla information för det blir lättare att förvalta det över tid, men det är ingenting GDPR tvingar oss till. Det är mer att vi ser typ, varför har vi 15 olika dropbox, om vi slår ihop det blir det mycket lättare för oss att säkerställa säkerheten.

35 JA: Det är ju också det här att för att kunna efterfölja, rätten att bli bortglömd och rätten att revidera data till exempel, måste ni veta var datan finns.

36 Informant 1: Det måste vi veta men ofta behöver vi inte ändra någonting om hur vi behandlar datan. Ja det kanske blir lite jobbigt om någon kommer och vill bli glömd eller vill bli raderad från våra system. I princip alla datasystem tillåter att vi gör det och gör dom inte

det så är dom designen på så sätt för att det finns en lag som gör att vi kan neka rätten till det. I alla fall hittills har det hängt ihop logiskt. Vi kan inte radera det för bokföringslagen säger det till exempel. Vi har en laglig grund för det så vi behöver inte anpassa system för GDPR. Sen kan vi säkert anpassa system så dom smidigare anpassas till GDPR. Skulle det vara så att vi måste lämna uppgifter kommer vi göra det manuellt. Sen om det är så att vi måste göra det så kanske det tar fem timmar per gång. Men det gör vi tills vi har fått tillräckligt många förfrågningar så att det inte är ekonomiskt försvarbart länge. I så fall är det aktuellt att ändra systemen så det här blir smidigare. Det är såhär många kunder har valt att hantera det idag. Vi kan uppfylla kraven men det måste inte vara smidigt.

37 JA: Nu har du varit inne på nästa fråga, kommer ni behöva lägga nya resurser på att tillmötesgå dom här nya kraven?

38 Informant 1: Dom flesta kunder jag har pratat med har resonerat så här: vi får se, vi gör så lite som möjligt nu up-front och är det så att massa kunder hör av sig får vi anpassa oss.

39 JA: Är man inte rädda för sanktionerna då?

40 Informant 1: Jo det är därför dom anlitar oss, så absolut är dom skrämda av sanktionsbeloppen. Men det går aldrig att vara säker på att man inte kommer få sanktioner. Det enda man kan göra är att göra så mycket som möjligt och känna att man har gjort det man kan.

41 JA: Så enligt datainspektionen så är det mer att man ska ha dokumentation om vad man har gjort och varför istället för att följa förordningen till punkt och pricka?

42 Informant 1: Som exempel kan man säga “okej vi har resonerat och kommit fram till att vi gallrar den här datan efter fem år för vi tycker det är rimligt” om sen datainspektionen kommer och menar på att det borde ske mer frekvent. Om vi då har dokumentation som visar att vi har valt fem år därför att och har ett resonemang runt det, kommer datainspektionen förmodligen ge oss en varning istället för en sanktionsavgift. Men om vi bara har satt fem år och inte haft något resonemang runt det så hade vi riskerat dom höga sanktionsavgifter.

Det finns sju grundläggande riktlinjer från datainspektionen och ignorerar eller bryter man mot dessa så är det dom höga sanktions beloppen som gäller. Men har du adresserat dom här principerna men datainspektionen inte håller med om detaljerna om hur du har gjort det så är det liten risk.

43 JA: Okej, sista frågan. Hur ser ni på ostrukturerade data och missbruksregelns borttagande?

44 Informant 1: Det beror på hur man ser på det. Men ja det är ett problem. Det är ändå någonting som ändå behöver göras enligt mig. Det är i grund och botten ett vettigt krav. Ur ett affärsperspektiv så är det egentligen fel att behandla slarvigt från början. Det är bra ur ett affärsperspektiv att vi tar kontroll över det på ett bättre sätt.

45 JA: Men du ser inte att det är ett problem att förhålla sig till?

46 Informant 1: Inte i vår verksamhet har jag inte uppmärksammat det. Allt beror på vad du har för ostrukturerad data. Möjligtvis kan det vara problem om man har saker som foton från mingel och foton från firmafesten förra året. Vad gör man om “Kalle” hör av sig och vill att

dom ska plockas bort. Det kommer såklart vara jobbigt. Men samtidigt är inte det verksamhetskritisk data. Medan annan ostrukturerad information som finns i offerter eller cv eller något liknande. Sådana saker innehåller mycket ostrukturerad data men det jobbar vi på att strukturera upp. Det är ändå någonting som kommer gynna oss ur ett affärsperspektiv.

47 JA: Okej då tackar vi så mycket för att du tog dig tid att svara.

9.2.2 Intervju 2 – Informant 2

Intervjuare - Edward von Essen (EV)
Sekreterare – Jens Andersson
Informant 2 - Junior Konsult. GDPR ansvarig internt, jobbar även med GDPR åt ett stort världsledande företag.

START

1 EV: Berätta lite om ditt arbete och var du är verksam just nu.

2 Informant 2: Jag jobbar som inom det interna GDPR-projektet och jag jobbar med GDPR ute hos kunder, jag jobbar med compliance, jag jobbar även som teamleader för våra cloud-arkitekter. Jag håller även på med studentprogrammet. Teknisk projektledare, jag gör allt möjligt.

3 EV: Du jobbar alltså med GDPR åt kunder?

4 Informant 2: Ja

5 EV: När började du arbeta med GDPR?

6 Informant 2: Jag började i princip direkt när jag fick en anställning här, efter att jag gick ut skolan. Så jag blev klar i juni och så började jag direkt. Jag började smått att arbeta med GDPR, då hade jag läst på lite innan jag kom hit och sen så kom jag in i det interna GDPR projektet och då drog de in mig i juli. Sen dess har jag jobbat med GDPR nästan 100 procent.

7 EV: Jobbar du med GDPR internt också?

8 Informant 2: Jag jobbar med GDPR internt för (O1) räkning och sen ute hos kunder också.

9 EV: Har du gått igenom någon utbildning inom GDPR?

10 Informant 2: Jag har gått igenom två olika utbildningar. Båda två har varit hos datainspektionen. Ena var i Stockholm, där det var inriktning på informationssäkerhet och mer hårdvara och sen så var det en annan som var mot offentlig sektor i Malmö.

11 EV: Är det ett måste att gå igenom en sådan utbildning?

12 Informant 2: Det var bara att du får alltid reda på smådetaljer som inte finns skrivet när du är på de där föreläsningarna eller utbildningarna. Så skapas det alltid diskussioner och så är det många branscher och sektorer som är där, så man får in sjukt mycket detaljer och insyn på området.

13 EV: Då kommer vi in på nästa fråga. I och med att GDPR inte har blivit implementerat så är lagen fortfarande tolkningsbar. Det finns inga prejudikat att gå efter. Har det funnits några svårigheter att tolka lagen för dig och kunderna du har arbetat hos?

14 Informant 2: Det man märker mer och mer just nu. Jag vet inte, får ni meddelanden från typ [företag] och [företag] där ni måste godkänna dataskyddsförordningen?

15 EV: Ja det har vi sett.

16 Informant 2: Man märker ju att organisationerna börjar förstå detta och lägga sig på en viss nivå om vi ska prata om detaljer och just nu har jag sett tre detaljnivåer. Det finns låg nivå, medelnivå och hög nivå. Låg nivå kopplas ofta till personer som tror att den nya förordningen kommer att hamna mellan stolarna och att det lixom är en grej som kommer och ingen bryr sig om det. Medelnivå är att man försöker förhålla sig till förordningen och försöker förstå sig på vad man bör göra för att vara safe, då är det oftast att man ska få loopan på plats och göra dpian på rätt sätt samt gå igenom och revidera pubavtal och vanliga avtal. När man kommer på hög nivå så är det att man börjar analysera på processnivå, alltså var i vår process kommer vi i kontakt med personuppgifter. Då försöker man analysera den processen eller subprocessen för att se vad man ska plocka bort för att inte komma i kontakt med personuppgifter eller hur man behandlar personuppgifter samt vad man bör ta bort för att det inte ska vara identifierbart till en person. Många idag lägger sig på en låg medelnivå för att man vet inte riktigt vad man ska göra. [Företag] är ett sånt exempel. De anger inte information i sitt användarvillkor vad informationen går, var den lagras. De skriver att underleverantören kommer att ta emot det, men man vet inte vilka och det ska de speca, speciellt när det är [Företag] som äger dem och all information går till erbjudanden. Säg att du till exempel köper C-vitaminer kommer du få erbjudande på apelsiner dagen efter lixom. Då behöver man gå och lägga sig på en högre nivå.

17 EV: Vilken nivå är du på?

18 Informant 2: Hos den kunden jag jobbar mest med är vi faktiskt på en medelhög nivå. Det har tyckts att vi är väldigt stränga med vad vi tycker och tänker. Det är bättre att utföra det hårt direkt än att falla tillbaka och behöva göra om. Internt hamnar vi på en låg medelnivå just för att det är mycket anställningsuppgifter. Man måste också kolla vilken bransch man jobbar i och hur det är. Sen är när det kommer till våra drift och förvaltningsprojekt så hamnar vi på en medelhög nivå där för att det blir ju viktigare. Så ja.

19 EV: Hur medvetna är anställda, låt säga både här och hos kund om GDPR generellt. Blir de utbildade i området?

20 Informant 2: Ja, utbildade blir dem. Vi har en portal vi har kört där alla anställda har fått gå in och svara på GDPR-uppgifter med utbildningsvideor och frågor och så. Sen kollar man inte upp så att alla har alla rätt. Det är inte heller rimligt men att alla har gjort den. Det är som awareness-videos.

21 EV: Är det både här och hos kunderna du arbetar?

22 Informant 2: Hos kund har de gjort så att vi har haft utbildningstillfällen och det har vi fortfarande. Stora organisationer så då har vi utbildningstillfällen hela tiden där de får svara på frågor. Vi har massa möten med dem för att vi ska kunna skapa den här ROPAN som det kallas, Record of Process activities. Och när vi sitter på dessa möten dyker det upp nya saker. När vi sen går tillbaka har de här föreläsningarna eller seminarietillfällena för anställda så dyker de upp ännu mer och då kan man i grupp diskutera det. Så de kör på en annan approach.

23 EV: Okej, jag tänker på de här nivåerna du pratade om. Är dessa på ledningsnivå?

24 Informant 2: Eh, ja det brukar väl oftast vara så. Det som ledning tar beslut för och vilken nivå ledningen lägger sig på sjunker ju neråt.

25 EV: Hur tror du att anställa uppfattar det hela?

26 Informant 2: Det är lite svårt att säga. Hos min kund nu så är det inte rent tekniskt bolag som vi, jag menar programmerare, tekniker bryr sig inte så mycket om regleringar och förordningar. Medan det företaget jag är hos dom är mer ett business-orienterat bolag där de hela tiden är i kontakt med personuppgifter. Så medvetenheten där är lixom. Det är obligatoriskt för dem att kunna förstå sig på det och vara medvetna om det. Medan här kan man ändå komma undan med det. Men jag tycker ändå att båda delarna, alltså här och hos kund, är det rätt hög medvetenhet faktiskt.

27 EV: När det gäller lagtolkning. Har det varit några problem att tolka hur den nya dataskyddsförordningen ska genomföras?

28 Informant 2: Det kopplas ju till de olika nivåerna jag har lyckats förstå mig på och det tar ju tid att förstå sig på dem. Sättet du tolkar förordningen på är sättet du läser den på, så beroende på vilken människa du är och vilken nivå du ligger på så kommer du att läsa den på ett annorlunda sätt. Jag har alltid sagt att förordningen ska läsas för vad den är. Det är många som försöker hitta en "workaround". Exempelvis organisationer som gör automatiskt opt-in om du inte hör av dig. Det är fel. Du ska själv välja att göra en opt-in. Så nej, förordningen är vag, det är den. Men det är också med vilka ögon du läser den. Väljer du att faktiskt läsa den för vad den är och ta den för vad den är och sluta tänka hur kommer jag runt detta så kommer du nog förstå dig på den.

29 EV: Har du upplevt att arbetet kring GDPR har påverkat på ett sätt som ni inte hade förväntat er? Vad har varit den svåraste utmaningen hittils?

30 Informant 2: Den svåraste utmaningen har väl varit att man ska göra så pass mycket, men det finns liksom inget tillvägagångssätt med förordningen. Det är en tolkningsfråga hur man ska göra saker oftast. Speciellt när det kommer till sårbarhetsanalysen. Sårbarhetsanalys har man gjort alltid, men för att man ska vara i linje det som datainspektionen vill att man ska vara så finns det lixom inte några riktlinjer heller.

31 EV: Vad sa du att de heter?

32 Informant 2: Sårbarhetsanalys. En dpia. Exempelvis om du har något system eller förvaltningsprojekt eller någonting så gör du en sårbarhetsanalys på det för att veta vilka gap det finns där, vilka risker det finns och då ska man ju stänga de riskerna. Det kan vara avtalsmässigt, det kan vara systematiskt, tekniskt, det kan vara organisatoriskt det kan vara att alla processer ska vara på plats. Det är något du måste ha för det mesta egentligen där du kan identifiera sårbarheterna. Om du har avtal på plats med kund och dig men inte har någon aning om vad sårbarheterna är, hur ska du då kunna uppfylla förordningen. Det kan vara att du inte har tekniska mekanismer på plats.

33 EV: Har det kostat mer än vad ni tänkt rent monetärt?

34 Informant 2: Pengamässigt har jag inte någon stor insyn på men jag tror att man lägger i linje med budget faktiskt. Sen så är det ju en sån här grej att det får kosta vad det kostar. Man måste få det på plats lixom. Har man skött PUL ordentligt från första början som Finland är ett fint exempel på. De har haft personuppgiftslagen som en sträng lag så de har inte lagt så mycket pengar på GDPR, för de ligger i princip i linje med allting. Då kostar det inte så mycket. Medan Sverige har använt missbruksregeln, vi har ju lyckats ta oss runt det mesta och då sitter vi i skiten lixom. Det mesta är offentlig information. Vi kan få ut information hej vilt medan om man kollar på våra grannar så är det inte alls så. De kan inte få ut information hela tiden. Danmark är inte alls så, de har inte samma utmaningar som Sverige har.

35 EV: Hos kund och här, har ni behövt göra stora förändringar i systemen?

36 Informant 2: Ehm. Hos kunden så ja. Rakt svar ja.

37 EV: På vilket sätt?

38 Informant 2: Det har inte funnits stöd för vissa grejer som förordningen säger att man ska uppnå. Det kan vara allt från att föra loggningsystem på rätt sätt. Alltså loggningsystem med datahygien så att det larmas så att du har en sportslig chans att höra av dig. Och säga till att det faktiskt har varit en breach. Förr när man utvecklade mjukvaror och system och databaser och man slarvade med att man skulle kunna plocka bort data för att data ska alltid ligga kvar och det är en grej som jag tror att de flesta har en utmaning med. Det ska gallras i alla led.

39 EV: Hur är det med hanteringen av ostrukturerad data? Hur stort problem är det?

40 Informant 2: Ostrukturerad data tar det till en annan del och det är det som har varit missbruksregeln. Att vi har kunnat använda oss av det i PUL. Ja, alltså oftast är ostrukturerad data en form av ramen av vår yrkesroll så att det faller inom jobb och inte att jag skriver personinformation om de kunderna jag är hos och egenskaper och så. Men visst, som teamleader skriver jag lite information om vad som har hänt och hur personer har reagerat. Men det är fortfarande inom min yrkesroll, jag måste ha det på något sätt. Det här med ostrukturerad data, det finns två sätt att se det på. Chefer måste ha det, folk måste ha det för att kunna ha koll på saker och ting, det kommer aldrig att försvinna, men det in i yrkesrollen. Men när det kommer till att man ska skanna i form av data analytics och BI en mängd ostrukturerad information för att strukturera upp det och för att kunna ta beslut till direktmarknadsföring och sälj så är det väldigt bra. Så det finns ju flera sidor av det här med ostrukturerad data. Väldigt långa svar, men det är också ett vagt ämne

41 EV: Vi pratade ju om det här med att ni har ändrat deras system. Tror du att det kommer behövas extra resurser för att liksom kunna tillmötesgå alla nya krav? Innan har man inte haft rätten att begära ut data osv.

42 Informant 2: Om det krävs extra resurser för att tillmötesgå det, är det det som är frågan? Det tror jag alltid. Man har nog inte beräknat. Man har inte vetat om arkitekturen man sätter ut i grunden på alla system. Men sen sätter man sig och allvarligt ska ta fram det för att få en förståelse för hur informationen går så inser man ju någonstans att det här var mer komplext än vad vi tänkte oss. Det har visat sig många gånger att det finns redudnant information, så om du plockar bort något så finns det kvar i systemet ändå. Så, det är nog den delen som har varit en väckarklocka och en sak man har tagit action på lixom. Ja. Det görs inte över en natt, det är så många saker som påverkas av det. Så ja, absolut krävs det extra resurser. Oftast så är det ett team som sitter med det då.

43 EV: Kommer ni ha en viss tid på er att anpassa er till den nya förordningen? Om du inte har uppfyllt kraven den 25:e så är det kört?

44 Informant 2: Efterlevnaden är ju en viktig del av detta. Du ska ha en efterlevnadsplan, actions och to-do lists på vad du ska göra och hur du ska fortsätta arbeta med det, vilket alla organisationer måste ha. Det är lixom ett krav att efterleva den nya förordningen. Bara för att det är den 25:e maj och du inte har uppnått vissa grejer så betyder det ju inte att du slipper undan. Om ni hade frågat mig vad det viktigaste är, och det är en personlig åsikt. De andra ni har intervjuat kanske tycker något annat. Men det viktiga för mig är att man ska ROPAN på plats, alltså Record of Process activities. Om ni hör av mig till mig och begär ut information så måste jag veta var informationen finns. Utan en ROPA är det omöjligt för mig att veta det, om du inte har teknisk telefonkatalog. Det vill säga, du skriver in namn eller personnummer så slås det upp var informationen finns. Men det tar tid att implementera det, det är ett halvårs implementeringstid. Tills 25:e maj så har du inte inte lyckats implementera det om du börjar idag.

45 EV: Tror du att det är en stor utmaning för många?

46 Informant 2: Ja. DPIAN, sårbarhetsanalysen och att gå igenom data processing agreements, som är dataavtal. Många har underleverantörer utan bra pubavtal. Många behöver instruktioner till sina pubavtal och ifall något händer och du ska bli frånlöst från allting. Processer, tillvägagångssätt hur ni hör av er till oss, hur vi hör av oss till er. De delarna måste komma på plats och allting som kommer på teknisk nivå. Loggsystemet kan jag nog prioritera, det är nog rätt viktigt att få ett loggsystem med larma och visualiserat så att man snabbt kan få en kännedom om någonting händer, för i slutändan är alla organisationers mål att inte läcka data. Det är ju det värdefullaste vi har, vi har inget annat, vi äger inget annat. För att ha en sportslig chans måste du ha något som larmar dig tekniskt, sen kan det tekniska alltid vara fel. Men har du det visuellt så kan du se att hårddiskarna jobbar extra mycket nu det finns ingen anledning för klockan är nio på morgonen. Då är det något som händer. Så ja, den delen är mycket viktig.

47 EV: Av de regler som den nya regleringen har framställt. Rätten att bli bortglömd, portabiliteten och att kunna ändra. Vilken är svårast att efterleva?

48 Informant 2: Portabiliteten är nog inte en biggie. Det är att man ska ha ett läsbart maskinformat och det har jag fått veta på datainspektionen att det är xml:er, textfiler. Så det ska inte vara något specifikt egentligen. Jag tror främst det är rätten att bli glömd, med tanke på att många organisationer har redundant information i sina databaser där det är kopplat på olika sätt, så om du plockar bort Edward von Essen så kan det komma in tre gånger till från ett annat håll. Då är det rätt tufft att kunna förhålla sig till det.

49 EV: Det är väl lite det att kunna identifiera var datan finns och strukturera upp? Gamla företag har väl lixom massa gammal data.

50 Informant 2: Under projektarbetet där du var, det är lixom ett legacyföretag. De har haft hur många system som helst och går i flera steg. De har diskuterat detta sedan 2016 och borde ha satt igång direkt. [Företag] är också ett sånt exempel, de har mycket information, sedan långt tillbaka, både på papper och digitalt.

51 EV: Kommer du bli en DPO?

52 Informant 2: Nej, i förordningen står det att det ska vara en person som har kunskapen och kompetensen. Jag kommer inte bli det, jag tror att vår CSO kommer att ta den rollen. Du kan bli certifierad DPO, alltså det finns certifikat att ta, men det är inte riktigt godkända certifikat. Det känns onödigt att lägga 15 000 på det. Nej, jag kommer inte bli DPO. DPO:n kommer att höra av sig till datainspektionen och till personer som blir berörda ifall information läcker. Deras jobb är att se till att det sköts på ett sätt att man har koll på avtalen om någon hör av sig och vill plocka bort mig, så ska de se till att personen blir borttagen.

53 EV: Tror du att det finns några utmaningar på lång sikt som GDPR kommer att medföra?

54 Informant 2: Utmaningsmässigt, ja. Att fortsätta ta förordningen på allvar när det kommer till efterlevnad. Det kommer att vara tufft att den 25 maj. Det är både en löningdag och en GDPR-dag lixom. Jag tror att gamla organisationer som inte förstår sig på detta kommer tro att datainspektionen ska glida in och börja inspektera bolaget, och om de inte gör det den dagen så är man lugn och så släpper man allt. Det är ett stort misstag om man gör det. Om man tror det. Det var en sak till jag tänkte på, men jag glömde.

55 EV: Känner du att det är något område som vi inte har diskuterat som är relevant?

56 Informant 2: Egentligen inte. Det dyker djupare mer och mer och man får ha ögon och öronen öppna. Man får försöka förstå sig på det. När jag gick i gymnasiet läste jag juridik så jag läste juridik i gymnasiet, vilket inte var på hög nivå men jag lärde mig iallafall att tolka lagar på rätt sätt och det har underlättat det här jävligt mycket. Jag har diskuterat med folk som bara har jobbat inom IT och gett sig på detta så märker man att man inte tar förordningen för vad den är.

57 EV: Det var det jag tänkte fråga, har du gjort detta arbete hos en kund?

58 Informant 2: Nej flera.

59 EV: Är det svårt för dem att förstå allvaret med den nya förordningen?

60 Informant 2: Hos vissa ja. Vissa förstår allvaret men de vet inte hur de ska göra, de vet inte tillvägagångssättet och de förstår sig lixom inte på varför det berör dem så mycket även om de vet att de berör dem. De vet inte hur de ska göra en sårbarhetsanalys, hur ska vi ha en ROPA. Räcker det med Excel lixom. Det gör det till en viss del men är du uppe i 110 system så bör du kanske kolla på ett systemstöd för ROPAN för då kanske det blir tufft med en efterlevnad i excel. Excel kanske håller i ett halvår. Vad händer om det blir en dump av datan eller av cloud-miljön ni har och excelen försvinner.

61 EV: De kunderna du har haft. Är det någon skillnad i storlek på dem?

62 Informant 2: Ja, och de är verksamma i olika branscher. Det är det som är mest tydligt.

63 EV: Ser du något mönster att stora företag är bättre förberedda.

64 Informant 2: Jag ser att utländska företag är bättre. Då är det alltså utländska företag inom EU. Då har man förhållt sig till dom personuppgiftslagar där man har varit mycket starkare än vad Sverige har varit. Sverige lever på transparens och är ett PK-samhälle, vilket är bra, inget illa menat. Men när vi har så hög transparens på allt vi gör och allting som handlar om information så är detta en utmaning. Vi kan få ut all information. Jag kan få ut all information om er två här och nu och det är på något sätt som att jag tar er integritet och här har vi en förordning som ska skydda er integritet. Hur gör vi det. Sen har man alltid kunnat referera till missbruksregeln. Intresseavvägning är ju helt okej i PUL. Man säger, vi har gjort detta av rent intresse, varför, jo men för att vi kände såhär. Det här funkar ju inte nu lixom. Nu är det samtycke eller en laglig grund från nationell nivå. Nationella lagar. Så ja, det är väldigt intressant. De som gör intresseavvägning för att behandla uppgifter kommer kunna göra det två tre gånger och sen kommer de få åka på någonting. Datainspektionen anställer 200 stycken och de kommer att gå hårt på detta.

65 EV: Ja, du har ju ändå varit där. Hur känns inställningen från datainspektionen? Vill de sätta dit någon tror du?

66 Informant 2: Datainspektionen är ju sjukt kritiskt mot våra myndigheter, alltså när det kommer till kommuner och skatteverket och sådär. De uppfyller inte alls de organisatoriska och tekniska kraven som krävs, vilket är skönt att de kritiserar dem och använder dem som dåliga exempel. Sen är det många kommuner som är under tillsyn. Det är främst genom personuppgifter och oftast om barn. Det är ju känsligare. Men stämningen där är ju väldigt tung i luften lixom. Det är inte ett glatt ämne för företagen. Jag tycker att det är kul för jag jobbar med det.

67 EV: Det känns ändå som att ni ligger i fas?

68 Informant 2: Jadå, vi kommer att klara det. Vi ligger i fas på den nivå vi har lagt oss på och det är samma hos kunden jag är hos. Vi kommer ju hinna. Vi har fått de viktigaste delarna på plats men när man är på datainspektionens utbildningar så fattar man ju att vissa jobbar med det och ansvarar för det som inte ska ha med det att göra. De förstår sig inte på det och det är synd, för det skadar deras organisation. Datainspektionen själva vet ju inte så jättemycket. De är jurister. De förstår sig inte på ren IT.

69 EV: Det är det som är det svåra känns det som. Lagen är där och finns tillgänglig men företagen vet inte hur de ska gå tillväga för att följa den. Har datainspektionen inga riktlinjer för hur det ska gå till?

70 Informant 2: Inte allt nej. Läser man förordningen på engelska och sen på svenska så är det två olika förordningar. Det är också en utmaning för att det svenska språket begränsar oss i att uttrycka saker som de gör på engelskan. Det engelska språket är mer övergripande naturligt. Exempelvis Joint-controller finns inte på det svenska språket och då är det något som faller bort och då översätter man det på ett annat sätt och då tolkas det på ett annat sätt. Svenska förordningen blir mer tolkningsbar. Man tolkar den på ett helt annat sätt. Så mitt tips oftast när folk ska sätta sig in i GDPR och börja jobba med det är att de läser den engelska samtidigt som den svenska för att kunna förhålla sig till den mycket lättare. Det är två olika artiklar i princip. Man förstår sig på det, innebörden, men i slutändan är det översatt på ett helt annat sätt. Det är kanske därför andra EU länder känns mer förberedda, för att de läser den på engelska. Det klart att det finns översättningar i de andra länderna också men engelsktalande organisationer läser den på engelska, och då tolkas den även på engelska och då är den lättare att förstå sig på hela förordningen. Så jag menar, om Gösta Andersson åtta år innan pension bestämmer sig för att jobba med detta och lär sig den på svenska blir det tufft. Gösta kan vara duktig, men han kanske inte riktigt förstår sig på det.

71 EV: Då tackar vi för oss.

9.2.3 Intervju 3 – Informant 3

Intervjuare - Edward von Essen (EV)
Sekreterare – Jens Andersson
Informant 3 - Arbetat med informationsstyrning de senaste 5 åren. Projektledare för GDPR-arbetet det sen juni 2017.

START

1 EV: Berätta om dig själv och vad du jobbar med?

2 Informant 3: I grunden är jag arkivarie, Så informationsstyrning är det jag jobbat med senaste 5 åren. Tidigare har jag varit inom kommun och det är så att vi är väldigt intresserade av informationen som hanteras i systemen. Så det hanteras rätt från början, att vi blir starkare i kravställning och så, vad för krav vi ställer på systemen. Det är det jag har jobbat med senaste åren. Så arkivarie idag är inte så som man tänker på arkivarie. Man tänker ofta på pappersarkiv och en fysisk lokal men det finns inte så många kvar. Många jobbar mer med digital styrning.

3 EV: När började du/ni jobba med GDPR?

4 Informant 3: Vi fick projektdirektivet fastställt i Juni 2017. Sen var inte första styrelsemötet förrän i september så det var lite seg start. Det var svårt att överblicka, det var svårt att stycka elefanten som alla säger inom GDPR. Men det var svårt från början.

5 EV: Hur hamnade det på dig?

6 Informant 3: Jag tror man såg så här, vi har inte en pott med projektledare som man kan välja mellan. Jag tror man såg en risk med att ta in någon externt. Då blir det inte den förankringen vi behöver i verksamheten. Och då landade det på oss, det var juristerna asså vårt personuppgiftsombud som först lyfte frågan att vi behöver dra i det här som ett projekt. Nätverket som det ser ut idag fungerar inte. Det han hade fungerade inte tillräcklig starkt för att dra i det här. Så då var det en diskussion, vi har haft tidigare mellan informationssäkerhet, regionarkivarie och personuppgiftsombudet. Det var hos juristerna diskussionen landade att vi behöver resurser till det här. Då var det rimligt att det landade på mig eller någon från vår enhet.

7 EV: Hur många är ni som jobbar med det?

8 Informant 3: Ja du, det är lite otydligt. Vi är fem stycken som sitter i en projektledningsgrupp som i princip jobbar heltid med detta, inte alla men nästan. Sen har alla förvaltningar egna grupper, vi är ju, hur många är vi nu, vågar inte svara på det, kommer svara fel. Men vi är rätt många förvaltningar, det är väl typ sju eller åtta. Dom har egna projektgrupper. Sen har vi några som inte direkt ligger hos oss, vi har några öar som ligger utanför som ändå varit med i projektet och har tagit del av metoder och så. Men som inte varit direkt involverade i projektet, bla revisionen, hälsostaden. Öar som ligger under fullmäktige, vi har ändå haft med dom i projektet. Lite on och off med folk. Vad vi har sett centralt, det här ju för stort för att vara ett projekt, snarare vissa har drivit det som ett programkontor. Så att vi har förvaltningen som har drivit frågor just vad det gäller inventeringen av personuppgifter, har dom drivit lokalt. Sen har vi haft en IT person med i projektledningsgruppen som har drivit det mot systemansvariga, så vi har haft dom spåren.

9 EV: Har du genomgått någon utbildning?

10 Informant 3: En väldigt kort, en dag har det varit.

11 EV: På datainspektionen?

12 Informant 3: Nej, vi har vårt personuppgiftsombud som är en fena på det här. Han har gått på datainspektionens utbildning. Han är inblandad, han har även varit där och tagit fram workshops så han är väldigt inblandad i det här. Så därför har jag lutat mig väldigt mycket på honom.

13 EV: Ofta kan man följa rättspraxis från gamla domar. Eftersom GDPR inte är implementerad än, finns det några utmaningar med att tolka lagen?

14 Informant 3: Vi har nog lämnat dom utmaningarna, det har varit så många. Vi har nog lämnat dom lite till sen. Vi har pausat det lite. Vi får chansa lite och lägga en ribba. Sen får rättspraxis visa om vi måste göra en ny avvägning. Till exempel information till den registrerade, ja på vilken nivå, det vet vi inte riktigt än.

15 EV: Vi har märkt att det är väldigt få som vet hur dom ska gå tillväga för att tillmötesgå kraven. Är det samma för er?

16 Informant 3: Så är det. Vi kollar hela tiden med vårt personuppgiftsombud. Det är jättesvårt för alla i förvaltningen vill ha, på projektledningen är det hårt tryck. Det är många som kommer till oss och undrar till exempel ”får jag göra så här”, ”ja kanske”. Det är väldigt svårt för oss att tolka, vi har försökt hjälpa och styra så mycket som möjligt. Men väldigt

mycket handlar om att dokumentera, hur vi tänkte. Så här tänkte vi, det kan vara fel men vi har iallafall tänkt, det är en jätteviktig del av processen.

17 EV: I vilken mån utbildas övrig personal i lagen?

18 Informant 3: Ja vad ska jag säga. Vad vi har gjort är, vi har tagit fram ett grundmaterial, informationsmaterial och det är det som förvaltningen, projektdeltagarna där sen har lutat sig mot. Vi har dragit på olika nivåer. Det har varit på koncernledningen hela vägen ner till arbetsplatsträffar. Dom flesta inom någon ledningsnivå förhoppningsvis har nåtts av den. Men det har varit en muntlig framställning. Dom har fokuserat mycket på att ni behöver städa tex. Vi har 70 miljoner filer på gång eller vad det nu kan va. Det är som en eskalerande bomb. Och det är det som varit en positiv grej med GDPR, alltså använda det som: ”ni måste ta tag i det här som ni kanske ändå innan borde haft koll på.” vissa förvaltningar har nog tagit det mer på allvar än andra. Men det har varit bra. Annars utbildning, vi hade från början tänkt ta fram en EU-utbildning, sen har vi haft mycket diskussioner, når vi rätt om vi tar fram en EU-utbildning. Når vi rätt om vi utbildar 34 tusen personer. Det kostar rätt mycket om man ska köpa in den. Landar vi helt rätt utifrån, vi vill inte hålla på att utbilda sjuksköterskor inom nåt dom inte behöver veta. Dom har så ont om tid och det är den utmaningen vi har. Det är skillnad på oss som jobbar här som kontorsråttor, vi har tid att gå utbildningar. Så vad vi kommit fram till nu, den här SKL utbildningen som förhoppningsvis blir klar inom några veckor, den kommer vi kunna luta oss mot. Vi har tagit fram lite diskussionspunkter till och, förslaget är att det ska visas på APT-möten så det når ut till alla medarbetare. Det kommer ta kanske 30 minuter av mötet där man kanske går igenom ett case som berör detta. Men detta har inte genomförts med alla än, men det är ambitionen. Alla kommer inte ha gått igenom en utbildning den 25 maj, så kan jag säga.

19 EV: Av de som jobbar med det här, dom sektioner det handlar om, hur är den generella attityden?

20 Informant 3: Det är nog lite olika, man kan tänka sig inom vården så är man jätte duktig på att tänka på patientlagen, så det har man i ryggmärgen. Sen är det allt det andra som faller utanför det här, där är det en utmaning. Inom vården tänker man att man är i hamn för man är duktig på att tänka på sekretess och dom delarna. Det vi försöker få in är det här med förbättringshjulet. Och det har inte riktigt landat i sjukvården, ja det är en sak att ni är duktiga på att förstå dom frågorna men ni måste ständigt bli bättre. Hur lyfter vi dom här behoven som finns. Men det är en jättestor utmaning för vården men det är en stor del av det här projektet tänker jag. Man måste lyssna på användarna och förhålla sig till lagen och centralt hjälpa till att ta fram rätt hjälpverktyg. Finns det en G-katalog där är det klart att du kan mata in känsliga uppgifter där, även om det inte är det bästa stället. Så ser man möjligheter så, man måste styra så mycket som möjligt. Vad var nu frågan från början? Nu svamla jag iväg.

21 EV: Attityd hos anställda

22 Informant 3: Attityd just det ja. Så vården är ett område för sig. Men attityden hos tex Skånetrafiken tar det superallvarligt. Men dom har också problem att ledningen inte lyssnar. Men det är svårt att säga hur känslan är. Men nu är det hett ändå. Vi har ett projekt och alla hör det här. Koncernledningen får den här informationen och har fått det ett par omgångar. Men risken är att, det har också börjat bli lite såhär: vi får väl vänta och se vad som händer. Dom kommer inte sätta dit oss, vi är ju offentlig sektor. ”Så det är lite olika.” Men det kommer bli hetare nu tänker jag. Så vi har chansen nu att göra så mycket som möjligt.

23 EV: Har ledningen aktivt arbetat med att förmedla hur man ska arbeta?

24 Informant 3: Nä det gör dom inte. Dom har utsett projektet då. Projektet har lite problem att nå uppåt. Dom som man tidigare haft utsett att jobba med dom här frågorna som kallas personuppgiftsföreträdare. Det kommer bli någonting annat nu, dataskyddssammordnare eller nåt. Dom har ofta varit väldigt långt ner. Ofta har det varit någon som varit sjukskriven sen får man 20 procent och det har varit för mycket på ens bord. Nu raljerar jag lite men att man har verkligen inte fokuserat och tagit det här på allvar innan. Så det är vår största utmaning nu att faktiskt få den nya organisationen att förstå hur mycket resurser en verksamhet som SUS med 12 tusen anställda behöver. Man kan inte ha en med 20 procent ska svänga det här med högerhanden och ska ha koll på allt det här. Det är en stor utmaningen men dom har drivit det i den nivån att dom utsett ett projekt i alla fall och det gjorde man ganska tidigt.

25 EV: Jobbar alla regioner självständigt eller finns det några direktiv ännu högre upp?

26 Informant 3: SKL, Sveriges kommuner och landsting har ett Eu-utbildnings forum där dom försöker dela dokument, men där är nästan bara frågor till dom bara. Men SKL har ”steppat” upp lite och har producerat en del styrande dokument. Sen är ett problem då att juristerna som sitter på SKL. Våra jurister som sitter här tycker att juristerna på SKL är lite slappa. Så det inte så att vi bara kan ta alla styrande dokument och ge dom en egen stämpling på dom med det vi tycker är viktigt att fokusera på. Sen har vi nätverk som vi haft hela tiden, med ett gäng andra landsting som vi försökt dela med oss av utbildningar, erfarenhet och styrande dokument men det är inte alltid så lätt för vi jobbar inte likadant.

27 EV: Nu när det gäller attityd och tolkning, vad har varit den svåraste utmaningen?

28 Informant 3: Vad som varit svåraste är hela tiden nivån, vilken nivå ska vi lägga oss på, vad är ”good enough”. Men det är inom alla delar av lagen. Jag tänker att vad som nyligen har varit en diskussion har varit det här med information. Hur mycket ska vi informera, hur generellt och hur breda kan vi vara. Sen tror jag att det inbyggda dataskyddet där har vi inte exakt landat i vad som behövs. Vi försöker mappa in. Vi har gjort en inventering med hundra frågor som du ska svara på utifrån ditt IT-system. Sen hur du har svarat är nästa steg vilka åtgärder som kopplats till det här. Mappningen där håller vi på med för att försöka guida systemansvariga. Men vad är det här inbyggda skyddet och vilken nivå ska man ligga på, det är inte lätt att förstå. Säger man såhär: ”det här är minimum nivå, ja då lägger man sig där”. Alla i sin roll, om man är systemansvarig ska man utifrån sin roll förstå hur man ska tänka på GDPR. Det är en jättestor utmaning.

29 EV: Har du märkt att GDPR på ett sätt som ni hade förväntat er?

30 Informant 3: Ja, den här ostrukturerade massan som är ostrukturerade filer som man kunde skita i innan. Där var vi lite, ska vi eller ska vi inte. Och då valde vi i höstas att vi kör på det också. Och det har inneburit att hela det här städfokuset. Vi har inte varit bra på att gallra, asså slänga grejer när vi ska. Så den här kopplingen som mitt yrke mycket handlar om, att försöka få människor att tänka på hur länge ni ska ha kvar uppgifter, ser du till att göra dig av med det och att tänka på säkerheten, skickar du med säker E-post. Att hela processen är tydlig, det har blivit mer aktuellt än vad jag trodde. Så det har varit en kul bieffekt men det har säkert haft med att göra att jag sitter som projektledare. Det tror jag dom flesta inte har gjort,

utan man försöker hitta generella behandlingar, till exempel, ekonomi någonting, och säger den behandlingar har vi. Medans vi har sagt då att varenda stackare ute i verksamheten ska leta reda på var det finns för personuppgifter, och då plötsligt började det,”shit vad vi har mycket grejer, vad ska vi göra.” Och det är något positivt i det också, då förstår man behovet av att skapa en struktur som funkar.

31 EV: Har det här arbetet kostat mer än vad ni förväntade?

32 Informant 3: Vi har en nollbudget i det här. Men det har ju kostat interna resurser. Skånetrafiken har valt att ta in en extern projektledare. Men vi har inte haft några, vi har haft några småslantar som vi pyntat ut på, nä det har knappt varit något. Vi har haft nollbudget så det har knappt varit nåt. Det här kommer ju sen. Det vi har gjort under året har i princip varit en jättelång förstudie, eller inte förstudie, vi har drivit det som ett projekt men det har varit lite grann som att vi kastat upp allt till ytan. Styrdokument och förarbete. Åtgärderna kommer inte ha åtgärdats till den 25 maj. Än så länge har vi bara tagit åtgärdsplanen. Sen har vi tänkt att förvaltningen ska ta hand om det. Organisationen som finns för dataskyddsfrågor ska kunna agera på det här. Och så skriver vi vår rapport med alla rekommendationer för hur arbetet ska fortsätta.

33 EV: Ja mycket verkar handla om efterlevnad. Men ni jobbar mycket med att arbetet inte slutar den 25 maj?

34 Informant 3: Ja jättemycket. Nu sist så beslutades det, ja det blev ett beslut att vi kommer skriva ihop vår rapport men styrgrupp och projektresurser finns kvar tills vi är säkra på att organisationen, där finns personer som tar vid, så en överlämning blir gjord ordentligt. Sen är det här med resursfrågor jättesvårt, speciellt inom vården. Så jag kan inte säga att vi kommer lyckas, det vet jag inte. Men till exempel habiliteringen har jobbat jättebra genom hela projektet, dom har utsett olika informationssäkerhetssamordnare. Vissa förvaltningar har bara haft en men dom har utsett ett gäng, om det är 20 stycken kanske. Och det är dom som ska jobba med GDPR inom projektet och det är dom som tar staffetpinne sen. Då har man en kontinuerligt där, överlämningen blir inget problem. Förvaltningen har gjort lite olika och det har vi haft svårt att styra centralt.

35 EV: Finns det andra utmaningar ur ett organisationsperspektiv som vi inte diskuterat?

36 Informant 3: Ja jag tänker på leverantörsfrågor. Det kommer inte vara lätt att personuppgiftsbiträdesavtal och vi har tagit fram en mall och vad som händer nu att leverantörer säger att här och där tycker vi såhär, vi har försökt att säga: ”vi måste hantera det här utifrån våra mallar.” det är vad projektet har sagt men sitter dom som faktiskt ska hantera det här i dialog med till exempel Microsoft. Och problemet är om man använder sig av någon annan leverantörs PUB-avtal då ska någon sitta och granska det. Om det duger eller funkar för oss. Det blir en stor utmaning, att kontrollera den, vi har inte jurister som växer på träd. Det är upp till den som sitter med upphandlingsdelen eller systemansvariga sitter med såna småavtal till leverantörer, så dom finns överallt. Och nu som vi upptäckte för ett tag sen, det är byggnader också. Alltså där behöver vi också kanske PUB-avtal, vi hyr byggnader av någon som har kameror eller våra RSID, våra kort för att logga i byggnader. Så det är rätt många PUB-avtal, så det är en stor utmaning för oss. Att den relationen ska fungera, det är inte bara ett avtal det ska ju vara vid en incident ha formulerats, vem ska agera och hur för att få den här 72-timmars delen och förmedla det till datainspektionen. Där är ju en bedömning, den processen är en utmaning.

37 EV: Har ni behövt göra omfattande förändring i era IT-system?

38 Informant 3: Det kommer det nog bli en del tror jag. Nu kanske man inte ska säga det här, det spelas in. Nä men det är så här, vi har en patientdatalag och vi har personuppgiftslagen. Hade det varit klockrent idag så hade det inte behövts en större anpassning till GDPR. Det är inte en så lång trappa. Men man kan tänka sig att vi har en del system som inte riktigt har varit där. Därför kan det bli så att flera anpassningar kommer behöva göras. Men det kommer absolut bli så, vi har tagit fram åtgärdsplaner och det kommer definitivt trilla in ändringar som kommer behöva göras. Men jag tror vi har också en gigantisk det här sammanhållen digital vårdjournaler, SDB-projekt som är upphandlat för hur mycket pengar som helst. Och där har man i hela upphandlingsprocessen tagit höjd för GDPR, GDPR är ett delprojekt i det. För att se till att GDPR och patientdatalagen uppfylls. Vi är på väg där, det är en långsiktig åtgärd att vi ser till att vi har system som är bättre anpassade till lagen. Vi sitter nu med många smådelar, nåt medicintekniskt, du kopplar upp dig, vi har det överallt. Den här IT-inventeringen som vi har gjort parallellt, har inneburit att, för det första bara vilka har vi. Vi känner till 850, och dom har vi inventerat 400 av, men alla innehåller inte personuppgifter. Dom flesta prioriterade system är inventerade utifrån det här frågeformuläret. Det betyder inte att vi har åtgärderna på plats. Sen har vi den här skugg-it, när verksamheterna inte går genom vår IT, då kör man någon annan, det kan vara allt från dropbox till”whatever”. Det är säkert tusen sådana, nu överdriver jag lite men ja. Där har också verksamheterna fått i uppgift, när dom letar på sharepoint och sånt så måste man även kolla om det finns egna IT-system eller applikationer som dom använder. Vi måste ha en central, har vi inte den centrala kollen så kan vi aldrig lyckas med informationssäkerhetsdelarna. Då är det kört. Det är en stor utmaning. Sen lagringar, backuper, raderas det verkligen om vi raderar och så. Jag känner att det inte är helt tydligt för mig, att vi har den kedjan. Men det har vi kanske om ni frågat IT-ansvarig.

39 EV: De här reglerna som finns: veta hur deras personliga data hanteras, rätta till uppgifter, rätten att bli bortglömd, portabilitet, tillsätta en DPO. Hur stort problem är det att förhålla sig till dessa regler?

40 Informant 3: Som rätten att bli glömd är en ganska liten utmaning, i vilka fall är det faktiskt relevant i en offentlig myndighet. Vi har bevarande och gallringsregler som gäller, vi bestämmer att det här ska bevaras i tre i verksamhet sen ska det skickas till arkiv. Det vi har varit dåliga på är att verksamheten har kvar information och skickar inte det till arkivet. Så där behöver vi bli bättre, men följer man bara dom reglerna så är, kan man inte inte bara säga:”jag vill bli glömd från arkivet” sen kan det nog vara vissa delar som vi blundat för. Jag tänker skånetrafiken är en sån. Dataportabilitet kanske är en fråga att hantera för dom. Men vi har lämnat den lite inom parentes. Våra jurister hävdar att det inte kommer bli aktuellt för oss. Dom andra landstingen har resonerat likadant. Att rätta till uppgifter, en stor utmaning är, vi hanterar det idag men det är det här med registerutdrag. För där har vi nu en manuell, jävligt seg process. Nä men om man:”hej jag vill ha mina uppgifter” då sitter det några centralt och handlägger och skickar ut till verksamheten sen ska verksamheten, skicka det och ja det är väldigt omständigt. Om vi får ett högt tryck den 25 maj, det oroar mig lite, att så här rättsaktivister, och kanske journalister kommer begära. Vi är jättebra rustade för det. Vi har i dagsläget ganska många system uppkopplade men inte alla fångar vi. Och det är lite hur vår IT-miljö ser ut, var drar vi gränsen.

41 EV: Vi har hört att många resonera likadant, det går och göra men det är inte enkelt. Blir det ett högt tryck så kommer man att ändra men i nuläget gör man inget.

42 Informant 3: Ja precis, idealet hade varit om vi hade kopplat upp oss mot alla system, problemet är ju att vi inte skriver in personuppgifter likadant i alla system. Hade man kunnat söka igenom alla system, så det är en framtidsdröm. I dagsläget har vi mellan 4-6 ansökningar om registerutdrag i månaden.

43 EV: Har ni behövt avsätta extra resurser för att tillmötesgå direktiven?

44 Informant 3: Ja det har vi, med tanke på hur många som ändå varit inblandade nu så, men jag hade önskat att det var ännu fler. Vi har haft svårt att nå vissa delar. Man förväntar sig att vi i projektledningen, vi är 4-5 stycken ska hantera dom här delarna, där man ska komma med direkta krav. Mycket handlar om att du i din roll ska förstå vad din roll innebär. Där känner jag att alla inte axlat eller förstått det ansvar som ligger på dom. Man vill gärna att någon annan ska ordna det, jurister eller vem det kan vara. Det har varit mycket mitt mantra nu att vi inte kan luta mot pär enbart. Om vi är 34 tusen anställda måste vi ha en organisation som fungerar, så att när han då, vilket förmodligen blir han, blir dataskyddsombud. Vi måste kunna hantera det här utan han, han ska bara gå in och tillsyna och kontrollera och råda oss, inte driva. Det är en stor karusell som sätter igång nu. Hur ser våra riskanalyser och mallar ut. Det är mycket sånt också nu. Hur kan vi som sitter centralt hjälpa till att göra det enklare, det är det vi får ta tag i nu.

45 EV: Sista frågan, den nya lagen kräver att man ska strukturera upp ostrukturerad data. Hur stort problem har det varit?

46 Informant 3: Alltså jag tycker ändå att det har varit, det har varit mindre av ett problem för när vi började prata om det, det är bara att följa bevarande och gallring det finns redan regler om det. Då har det varit en stor okunskap i organisationen att man inte vetat att det finns dom här reglerna att förhålla sig till. Men utmaningen som jag ser nu är att framöver att dom här reglerna fortfarande fortsätter finnas med i ens närhet. Det är ofta så här: Man har dålig koll på hur olika processer ser ut. Hur får vi ett mer aktivt stöd i arbetet. Det blir en utmaning att få till det. Vi har lyckas att nå ut med att det ostrukturerade ska hanteras, man ska inte slänga allt man har, för det är så vissa tänker ”nu kastar vi alla personuppgifter”.

47 EV: Tack för alla bra svar!

9.2.4 Intervju 4 – Informant 4

Intervjuare – Jens Andersson (JA)
Sekreterare – Edward von Essen
Informant 4 – IT-service management konsult. Lång erfarenhet av informationshantering och informationssäkerhet.

1 **JA:** Berätta om din position och vad du arbetar med.

2 Informant 4: Jag är It -service management konsult på (O4) och har jobbat här i 1.5 år. Jag är nu lite ansvarig för det här med GDPR både internt för syd och har haft den rollen i 6 månader strax innan årsskiftet. Och innan dess har jag jobbat rätt mycket med just hantering av information och informationssäkerhet och lite andra projekt. Så GDPR mest.

3 JA: Var det några som jobbade med GDPR här innan du kom, alltså för ett halvår sen?

4 Informant 4: Nja, jo, nja vi har ju en avdelning med IT och informationssäkerhetsfrågor. Sen är det även jurister och folk från det hållet till IT-säkerhet i stort.

5 JA: Men om vi går tillbaka till (O4), vad gör ni bara kort?

6 Informant 4: Vi är ju kända för att sälja produkter till företag. Det inkluderar hårdvara, mjukvara, nätverkslösningar och Cloud osv. Sen har vi också en konsultverksamhet där vi säljer olika konsulttjänster till företag. Vi är växande och har mycket rekrytering av konsulter och vi behöver alltid mer.

7 JA: För GDRP-arbetet, har ni interna jurister här också?

8 Informant 4: Ja det har vi, både central och inom kontoret här som är insatta i de juridiska delarna av GDPR.

9 JA: Har du fått någon utbildning?

10 Informant 4: Ja vi har internutbildning i GDPR centralt som innefattar elva lektionstillfällen där man går igenom GDPR och vad det innebär och vilka krav som ställs och vilka utmaningar som finns att hämta. Det är en allmän utbildning för alla anställda men det är inget krav på att man måste ta den, utan mer av frivillighet. Samtidigt så finns det ju ett slags krav på att man är införstådd på vad GDPR innebär och vilka krav det ställer på oss och företag för att efterleva den.

11 JA: Har du varit på dataskyddsinspektionen och fått utbildning där?

12 Informant 4: Nej inte i GDPR, men jag har ju gått ett antal utbildningar i informationssäkerhet i riskhantering osv, men GDPR-utbildningen har bara skett internt.

13 JA: Då går vi till våra problemområden. I och med att GDPR är implementerat, har det funnits några problem att tolka lagen?

14 Informant 4: Både ja och nej. De flesta utav oss som jobbar med detta har ju ganska gedigen kunskap jämfört som det har varit tidigare med PuL och alla de andra lagarna i och med vad GDPR kommer att ersätta. Så där har det varit ganska mycket i alla led och även från huvudkontoret där de säger vad vi ska tänka på. Sen är det såklart så att vi har kontakt med våra kunder på ett antal olika företag så uppstår det ju alltid ett antal frågor från dem. Hur, vad och varför. Där är det lite svårt ibland att lixom att svara på alla dessa frågor. Där är det även praktiska saker som till exempel hur man ska göra med backup hur ska vi göra med spamfilter och hur ska vi göra med fotografier. Så där är det alltså rätt mycket praktiska delarna och där blir det svårt ibland.

15 JA: Det kommer till nästa fråga. Både här och hos kund, hur känns den generella attityden till den nya förordningen?

16 Informant 4: De flesta förstår ju och de flesta varför detta måste finnas på plats. I något slags missbruk eller har man lixom inte gjort det här ordentligt så kan det bli dyrt, till exempel den här sanktionsavgiften. Sen finns de ju de som säger att de redan har ju redan fixat allt idag enligt PuL och vi har ju det och det och måste vi verkligen göra det här. Måste det göras och

måste det finnas lixom. Lite olika åskiter från företag till företag. De flesta har ju ändå förståelse.

17 JA: En avvikande fråga, vi har intervjuat region skåne och där var det väldigt svårt att nå uppåt för ledningen var negativt inställda. Är det samma problem för era kunder?

18 Informant 4: Aa, större kommuner och regioner har inställningen att de är så stora att de aldrig kommer att bli fällda eller bli granskade. Vet inte vad man ska säga om det.

19 JA: Vi går över till ledningen på ATEA. Har ledningen arbetat aktivt för att förankra vad GDPR kommer att innebära

20 Informant 4: Jag kan inte svara för alla kontor och alla regioner. Centralt har de förmedlat vad som skall göras och vad som måste finnas på plats innan 25:e maj. Vi ska ju iallafall försöka se till att det mesta finns på plats.

21 JA: På vilket sätt har detta gjorts?

22 Informant 4: Vi har ju haft rätt mycket interna möten och fått mycket information samt genomgått interna utbildningar bland annat. Vår VD har också skickat ut information om vad som skall göras och sen har det gått till regionchefer och alla pratar mycket om GDPR. Varje region har en GDPR ansvarig som jobbar med detta. Hela koncernen har tagit fram policys för alla regioner att följa

23 JA: Har ni upplevt att arbetet med GDPR har påverkat er på ett sätt som ni inte hade förväntat er?

24 Informant 4: Ja det skulle jag vilja säga. Människor som tidigare inte har pratat om GDPR och IT-säkerhet har börjat prata mer om det och fått större förståelse och uppmärksammat för att det är viktigt för oss och för kunder. Det här är något som vi aktivt måste jobba med och inte bara till den 25:e maj utan man måste aktivt fortsätta för att ha koll på det här.

25 JA: Det är något som många har tryckt på, att man ska vara klar den 25:e maj och sen är det klart.

26 JA: Har arbetet kostat mer än vad ni tänkt er både internt och hos kund?

27 Informant 4: Inte vad vi har märkt iallafall. Inga jättestora kostnader iallafall.

28 JA: Har kunderna ni är hos varit medvetna om hur mycket hjälp de har behövt?

29 Informant 4: Det finns ju kunder som underskattar behovet och tror att det bara är några timmars som behövs. Sen har det visat sig att det är ganska djupgående arbete som behövs. I både timmar och kostnader. Jag vill inte påstå att det är många som har det problemet. De flesta är nog medvetna om lixom vilken typ av problem de har och var de ska börja någonstans.

30 JA: Vilka utmaningar för själva organisationen tycker du att arbetet med GDRP har medfört?

31 Informant 4: Största utmaningen som jag har sett är nog för säljorganisation där man tycker att främst det här med DPA.er och avtal. Måste vi verkligen jobba med sånt, vi vill ju bara sälja. Det är den attityden som man har. Där får man ju också gå djupare, se det som en bilaga och lägg den vid sidan av kundavtalet. Vi skakar hand om detta och tar hand om detta. Det måste följas. Men det är inte många timmars extraarbete ändå att få det på plats.

32 JA: Måste de avtalen vara inrättade innan 25:e maj?

33 Informant 4: Ja alltså vi har ju numera DPAer som standard i alla avtal som går ut. Men sen är det ju gamla avtal som är skrivna innan årsskiftet som vi måste gå igenom och komplettera med DPAer och det har varit lite knepigt. Varför måste vi göra det här.

34 JA: Många menar att det inte handlar om tekniska aspekter utan snarare dokumentation och organisatoriskt. De vet inte vilken nivå de ska lägga sig på och så lägger de en ribba och väntar och ser. Märks det hos er?

35 Informant 4: Vi är ju ett IT-företag så jag vill påstå att vi har varit mer beredda på GDPR än vad många av våra kunder är. Så, där får man föra dialog om att det från ett organisatoriskt perspektiv krävs mycket från er. Vissa av er måste ha dpoer och andra som har det formella ansvaret för att lagen efterföljs. Mycket djupgående arbete hos många kunder.

36 JA: Det här med att man måste dokumentera och spara uppgifter, känner ni att era kunder fattar varför de måste göra den här förändringen?

37 Informant 4: De flesta gör ju det, sen är det ju också rätt stora variationer i inställningen hos olika företag och kommunen. Det finns ju företag som är hysteriska, vad är det som gäller. De täpper till all data och tar bort mycket information. Så fort någon skickar ett mail så tar de bort det från utkorgen. Där får man gå in och säga att det inte riktigt är den typen av saker som GDPR som GDPR tar upp. Sen finns det folk som har rätt dålig attityd, alltså att de har redan PUL och kan följa missbruksregeln. Det räcker inte. Missbruksregeln kommer att försvinna, och då får man berätta för dem att de måste ha ett annat tänk och en annan approach till det här. Så att det skiftar så mycket i dialogerna som man har mellan företagen. Men dokumentation får man trycka på. Det är viktigt att man har de processerna och ansvarsområden som krävs för att efterleva förordningen. Man skall åtminstone visa vilka intentioner man har haft med att följa förordningen.

38 JA: Finns det fler utmaningar som vi inte har pratat om som du tycker är svåra?

39 Informant 4: Det är ju främst skillnaden i attityderna hos kunderna.

40 JA: Både här och hos kund, har ni behövt göra omfattande förändringar i IT-systemen?

41 Informant 4: Nej det har vi inte, det handlar mer om att sålla bort data.

42 JA: Om vi pratar om de här konkreta reglerna. Hur väl förberedda är företag på det idag? Har de funktionaliteten att ta bort någon om man vill?

43 Informant 4: De flesta kunderna har ju det. Men sen finns det ju andra som har väldigt spretig miljö och inte har koll på sina system. Där får man gå in och aktivt hjälpa dem. Sen gäller lixom det här med förståelsen vad det här kommer att innebära. Att användaren har rätt att granska, rätt och ändra på information osv. Här är nog de flesta införstådda med det tycker

jag nog. Sen finns det ju företag och kommuner där man försöker lösa detta med automatisering, att användaren själv ska kunna gå in via en webbportal och begära att få bli bortglömd från register osv. Det är ju lite skillnad på mognadsgrad från varje företag.

44 JA: Har ni behövt avsätta mycket resurser för GDPR-projektet?

45 Informant 4: Ja jo det gör vi ju. I hela landet har vi ett projekt för GDPR och just DPAer och att de skall skicka ut det till kunder. Och grupperingen av männsiksor som jag ingår i har skapats för detta arbete det är många inom ATEA som jobbar med detta. Jag jobbar 50-70 procent med detta, sedan har jag lite andra projekt och uppdrag som jag jobbar med.

46 JA: Kommer ni vara helt klara den 25:e maj?

47 Informant 4: Jag är inte helt övertygad om att vi kommer vara klara till den 25:e maj, men till årsskiftet kommer vi vara klara tror jag. När jag säger så menar jag hela koncernen i Sverige. För (O4) syds räkning har vi nog rätt bra koll så där skulle jag nästan kunna garantera att vi är klara till den 25:e maj. Jag hoppas och tror det. Det känns som att det kommer vara klart till den 25e maj.

48 JA: Hur kommer arbete se ut för att efterleva den nya förordningen?

49 Informant 4: 26:e maj kommer vi att börja med kontroller och stickprover för att se hur arbetet går. Det är bättre att vi gör det först än att datainspektionen kommer och knackar på dörren. Vi börjar därför med granskningsarbetet den 26:e maj redan för att se om allt ligger på plats. Efter 25:e maj kommer det bli lite högre grad av prioritet. Vi får ju trycka på att en grundstomme måste finnas då. Det som inte finns på plats då kräver ju en liten högre urgency att få på plats så för att inte riskera problem när datainspektionen kommer och knackar på dörren. För då är det på företagens egen risk mer eller mindre. Om saker inte finns på plats då sitter de i skiten.

50 JA: Den nya lagen kräver att man ordnar upp i ostrukturerad data? Hur stort problem är det?

51 Informant 4: Vi behandlar ju väldigt mycket data men jag tror vi har bra rutiner för att hantera ostrukturerad data. Ute hos kunderna är det lite mognadsgrad på det här. Hos vissa kunder när man pratar om metadata så skakar de nästan på huvudet och frågar vad det är och vad man menar. Så där krävs det ju insatser för att få dem att förstå det här samt skapa rutiner och processer så att man lättare kan efterleva efter den 25:e maj.

52 JA: Hur kommer ni agera för att vara effektiva i förändringsprocessen?

53 Informant 4: Mycket handlar ju om att få dem att förstå vad som ska göras. Det handlar ju mycket om personkemi och vilka attityder som finns hos företagen. Men vi kan ju bara dra det hela till en viss gräns och sen får kunderna ta över. Vi kommer finnas till hjälp för kunderna men dom kommer få göra mycket av det aktiva arbetet. Många av våra kunder är mest rädda för att det kommer komma en hop med människor som kommer att kontakta dem för att få data om dem raderad och för att veta vilken information som finns. Det tror många av våra kunder kommer att skapa kaos, de har inte resurserna och kommer inte hantera mängden av människor som vill göra saker. Jag tror de flesta fullständigt kommer att skita i det.

54 JA: Tack för bra svar!