LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Dataportabilitet – en utmaning i en era av GDPR

En undersökning om vilka utmaningar verksamheter ställs inför för att kunna erbjuda dataportabilitet i samband med införandet av GDPR.

Kandidatuppsats 15 hp, kurs SYSK16 i Informationssystem

Författare: Edvin Blomberg
Jesper Fransson

Handledare: Benjamin Weaver

Examinatorer: Anders Svensson
Umberto Fiaccadori

Dataportabilitet – en utmaning i en era av GDPR: En undersökning om vilka utmaningar verksamheter ställs inför för att kunna erbjuda dataportabilitet i samband med införandet av GDPR.

FÖRFATTARE: Edvin Blomberg och Jesper Fransson

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

FRAMLAGD: maj, 2018

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 90

NYCKELORD: Dataportabilitet, GDPR, Personuppgifter, Utmaningar, Interoperabilitet

SAMMANFATTNING (MAX. 200 ORD):
I och med införandet av EU:s nya dataskyddsförordning (GDPR) kommer rättigheten till dataportabilitet bli verklighet. Dataportabilitet syftar till att användare fritt ska kunna plocka ut sina personuppgifter från IT-miljöer och ha dessa till eget bruk eller överlämna till andra tjänster eller IT-miljöer. GDPR har sett till att verksamheter kommer få ta ställning till utmaningarna som det nya dataportabilitetskravet medför genom flera olika aspekter. I studien undersöker vi vilka tekniska och organisatoriska utmaningar verksamheterna ställs inför för att kunna bemöta det nya dataportabilitetskravet. Detta via kvalitativa intervjuer med informanter inom olika sektorer som har erfarenhet inom förändringsarbete mot GDPR och dataportabilitet. Det visar sig av studiens resultat att merparten av verksamheterna stött på flertalet tekniska och organisatoriska utmaningar. Några svårigheter är att identifiera och extrahera personuppgifter ur sina system men också att förstå och motivera syftet bakom kravet samt hos vem ansvaret ligger. Dock anser verksamheterna inte dataportabilitetskravet som något väldigt aktuellt för just deras verksamhet då de räknar med att hantera ett fåtal dataportabilitetsbegäran. Därav har dataportabilitetsfrågan nedprioriteras i verksamheterna och endast ett fåtal verksamheter har vidtagit åtgärder för att möta dessa utmaningar.

Innehåll

Figurer

Tabeller

1 Introduktion

I detta kapitel kommer studiens bakgrund, problemområde, forskningsfråga, syfte och avgränsningar behandlas.

1.1 Bakgrund

Under de första månaderna av 2018 har skandalerna kring Facebook och Cambridge Analytica varit frekventa nyheter världen över. Upp emot 87 miljoner Facebookanvändares uppgifter kan olovligen ha hamnat hos det brittiska analysföretaget Cambridge Analytica utan att användarna vetat om det (Sveriges Radio, 2018). I samband med nyheterna sjönk Facebooks börsvärde med motsvarande 501 miljarder kronor (The Guardian, 2018) bara på några få dagar och hashtaggen #deleteFacebook (The New York Times, 2018) blev populär på flertalet sociala medier. Detta exempel på vårdslös hantering av personuppgifter och integritetskränkning är något som den nya dataskyddsförordningen GDPR ska försöka hämma samt ge EU-medborgare bättre integritetskontroll.

Den 25 januari 2012 föreslog Europakommissionen en genomgående reform av EU:s dataskyddsregler genom att presentera ett utkast till den nya dataskyddsförordningen, även kallad General Data Protection Regulation - GDPR (EDPS, 2018). GDPR är en ny reglering rörande bearbetning och hantering av personuppgifter som ska tillämpas av samtliga medlemsländer i den Europeiska Unionen. Efter fyra år av revideringar och förändringar blev GDPR accepterat av EU den 6 april 2016. Där bestämdes att GDPR ska träda i kraft den 25 maj 2018. Syftet med den nya förordningen är att rikta sig till att öka medborgarnas integritet genom att förbättra och skydda deras medborgerliga rättigheter och friheter.

En av nyheterna i den nya förordningen är rätten till dataportabilitet (Datainspektionen, 2017i). Detta innebär att en person som delat sina uppgifter med en verksamhet får rätten att ta ut sina personuppgifter vilka de har tillhandahållit den personuppgiftsansvarige (Datainspektionen, 2017a). Vidare får den registrerade överföra dessa uppgifter till en annan personuppgiftsansvarig utan hinder. Den enskilde EU-medborgaren kommer då ges möjligheten att t.ex. överföra delar av sina uppgifter från tjänster som Facebook till konkurrerande sociala medier med högre integritet eller flytta historik från en streamingtjänst till en annan.

Dataportabilitet syftar till att den registrerade fritt ska kunna plocka ut sina uppgifter och ha dessa till eget bruk eller överlämna till andra tjänster eller IT-miljöer (Datainspektionen, 2017b). Grundtanken är att dataportabilitetskravet ska uppmuntra till innovation och konkurrens inom EU:s medlemsländer och förhindra inlåsning av personuppgifter.

Härigenom kan rätten till dataportabilitet komma att sätta press på verksamheter att utveckla sina tekniska lösningar och interna processer men framförallt etablera samarbete och upprätta standarder mellan verksamheter inom samma bransch eller sektor (Datainspektionen, 2017b).

1.2 Problemområde

Föreskrifterna i GDPR är teknikneutrala (av skäl nr 15 som anges i GDPR 2016/679 den 27 april 2016) för att undvika teknikberoende och inlåsning, vilket ska förhindra att reglerna kringgås. Eftersom lagen är teknikneutral finns inte heller några föreskrivna format för personuppgifter som verksamheter måste använda sig av, utan formatet bör vara "i ett strukturerat, allmänt använt och maskinläsbart format" (Datainspektionen, 2017a). Vidare förespråkar förordningen interoperabilitet, att verksamheter inom samma sektor eller bransch ska samarbeta för att utveckla branschstandarder och standardformat både på teknisk och organisatorisk nivå (Datainspektionen, 2017a). Beroende på vilken sektor verksamheten opererar inom kommer omfattningen av dataportabilitetskravet se annorlunda ut, men det grundläggande konceptet är detsamma.

Då lagen presenterades först 2016 har verksamheter haft 2 år på sig att vidta åtgärder att åtfölja GDPRs föreskrifter. Redan då höjdes varningsflagg i en artikel av Tankard (2016) där han menar att omställningen och anpassningsarbetet för verksamheter borde börjat redan då. Även en undersökning gjord av RSM (2017) i november 2017 där 400 företagsledare från europeiska företag deltog, påvisades att endast åtta procent av företagen var redo för införandet av GDPR. I samma undersökning fastslås även att var fjärde företagsledare inte var medveten om vad lagen innebar och vilka anpassningar som måste till (RSM, 2017).

I händelse av att en verksamhet bryter mot en eller flera av förordningens regler kan verksamheten bli ålagd av att betala en sanktionsavgift på upp till 4 % av den årliga omsättningen (Datainspektionen, 2017i).

Den data som verksamheter är skyldiga att erbjuda vid en dataportabilitetsbegäran är enbart data som användaren själv tillhandahållit (Datainspektionen, 2017). Verksamheter måste då själva avgöra vad de anser är tillhandahållen data och samtidigt uppfylla användarens förväntningar på vad för slags uppgifter det är. Uppgifterna måste också identifieras och extraheras, vilket kan skapa problematik när verksamheter ibland använder flertalet olika system som sträcker sig över flera avdelningar.

Då lagen inte exakt preciserar hur en verksamhet ska besvara en begäran om dataportabilitet finns en viss förvirring hos verksamheter. Internetleverantören Banhofs VD Jon Karlung sa sig frågande i en intervju i DFAnalys (2017):

> *"– Till exempel hur möjligheten till dataportabilitet ska fungera i praktiken?"*

Därigenom har rätten till dataportabilitet sannolikt tvingat verksamheter att genomföra tekniska och organisatoriska förändringar utifrån en lagstiftning som kan anses otydlig och abstrakt. Vidare måste verksamheter förstå sina kunder och veta vilka uppgifter som finns och var dessa uppgifter finns lagrade i verksamhetens system. Samtidigt uppmuntrar lagen till branschsamarbete, ofta mellan konkurrenter. Utmaningar som kan anses högst komplexa för verksamheterna.

1.3 Forskningsfråga

Vår forskningsfråga syftar till att identifiera vilka tekniska och organisatoriska utmaningar verksamheter ställs inför för att kunna erbjuda dataportabilitet i enlighet med den nya lagstiftningen GDPR. Den empiri som insamlats syftar inte till att utgöra en manual för hur man möter nya lagkrav, utan ska försöka bidra med insikter för olika verksamheters utmaningar. Nedan följer vår valda forskningsfråga:

Vilka tekniska och organisatoriska utmaningar ställs verksamheter inför för att kunna erbjuda dataportabilitet i samband med införandet av GDPR?

1.4 Syfte

Syftet med vår studie är att, genom en kvalitativ intervjustudie, undersöka vad företag själva anser är deras tekniska och organisatoriska utmaningar med att följa det nya dataportabilitetskravet. Studien syftar även till att försöka identifiera vilka åtgärder verksamheter vidtagit för att kunna svara på en dataportabilitetsbegäran. Studien kommer fokusera på vilka tekniska och organisatoriska förändringar som har skett och kommer att ske inom verksamheterna.

Syftet med vår studie är även att vi förhoppningsvis kan bidra med insikter kring vilka utmaningar olika verksamheter ställts inför för att kunna erbjuda dataportabilitet.

1.5 Avgränsningar

Inga egna tolkningar av GDPR kommer göras då vi kommer använda oss av sekundärkällor, såsom artikel 29-gruppens riktlinjer kring dataportabilitet samt datainspektionen. Vidare kommer inte uppsatsen avse att återge en verksamhets officiella åsikt kring vilka utmaningar som finns kring dataportabilitetskravet, utan snarare intervjuobjektens personliga åsikter kring utmaningarna. Specifika branschförordningar kommer inte tas i beaktning i denna uppsats.

2 Litteraturgenomgång

I detta kapitel behandlas litteratur som är relevant för studiens forskningsfråga. Litteraturgenomgången mynnar sedan ut till den presenterade undersökningsmodellen, som sedan ligger till grund för att skapa intervjufrågorna i studien. Inledningen av kapitlet syftar till att ge läsaren en uppfattning om GDPR och framförallt dataportabilitet, och även förklaring av sekundärkällor. Vidare introduceras teorier kring interoperabilitet som är en av grundtankarna kring dataportabilitet och GDPR som helhet. Därefter introduceras läsaren till de tekniska riktlinjer som GDPR förespråkar såsom Privacy by Design samt tekniska format på uppgifter. Slutligen presenteras en genomgång om verksamhetsförändringar ur ett processorienterat perspektiv för att ge läsaren en inblick kring denna aspekt.

2.1 Dataportabilitet i GDPR

2.1.1 General Data Protection Regulation

Den 25 maj 2018 kommer dataskyddsförordningen, även kallad GDPR, börja gälla. GDPR är en lag som reglerar behandling av personuppgifter och syftar till att stärka och skydda den enskilde EU-medborgarens rättigheter och integritet (Datainspektionen, 2017h). Lagen kommer börja gälla direkt i alla EU:s medlemsländer och ersätter då tidigare nationella lagar (Datainspektionen, 2017i). GDPR har även som syfte att skapa en enhetlig och likvärdig nivå för personuppgiftsskydd inom EU och se till att det fria flödet av uppgifter inte hindras (Datainspektionen, 2017h). Mycket i GDPR liknar de lagar och regler som fanns i nuvarande Personuppgiftslagen (PuL) från 1998 men med vissa nya viktiga inslag såsom rätten till dataportabilitet (Datainspektionen, 2017i).

2.1.2 Artikel 29-gruppen

Artikel 29-gruppen består av representanter för samtliga dataskyddsmyndigheter i EU:s medlemsländer samt representanter för den europeiska datatillsynsmannen och EU-kommissionen (Datainspektionen, 2017j). Denna oberoende arbetsgrupp har som en av flera uppgifter att reda ut frågor som rör tillämpningen av dataskyddsdirektivet 95/94, och att vidare ge råd, stöd och riktlinjer för andra föreslagna åtgärder med avseende till behandling av personuppgifter såsom GDPR (Datainspektionen, 2017j). Artikel 29-gruppen har genomfört åtskilliga vägledningar för hur bestämmelserna i GDPR ska tolkas och genomföras rent praktiskt (Datainspektionen, 2017j).

2.1.3 Personuppgifter

GDPR är som tidigare nämnt en förordning som reglerar behandling av personuppgifter. Med personuppgifter åsyftas olika slags upplysningar som avser en identifierad eller identifierbar fysisk person. Uppgiften anses vara en personuppgift om den enskilt eller i kombination med andra uppgifter kan kopplas till en levande fysisk person (Datainspektionen, 2017g). Personuppgifter kan vara typiska uppgifter såsom namn, personnummer och adress men även bilder

och ljudupptagningar av individer kan anses vara uppgifter. Ytterligare personuppgifter kan vara krypterade uppgifter och olika slag av elektroniska identiteter såsom cookies och ip-nummer (Datainspektionen, 2017g).

Personuppgifter definieras enligt artikel 4.1 i GDPR 2016/679 av den 27 april 2016 som:

"varje upplysning som avser en identifierad eller identifierbar fysisk person [...], varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet "

2.1.4 Dataportabilitet och dess syfte

En av nyheterna som presenteras i GDPR är artikel 20 vilket innebär rätten till dataportabilitet. Denna nya rätt ger de registrerade större inflytande över sina egna personuppgifter genom att underlätta förflyttning, kopiering och överföring av personuppgifter från en IT-miljö till en annan (Datainspektionen, 2017a).

Dataportabilitet definieras enligt artikel 20.1 i GDPR 2016/679 av den 27 april 2016 som:

"Den registrerade ska ha rätt att få ut de personuppgifter som rör honom eller henne och som han eller hon har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format och ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan att den personuppgiftsansvarige som tillhandahållits personuppgifterna hindrar detta [...]"

Syftet med dataportabilitet är att göra det möjligt för EU:s medborgare att få ut, samt vidareutnyttja de uppgifter de själva har bidragit med till en IT-miljö. På så sätt ges EU:s medborgare möjlighet att använda dessa uppgifter till eget bruk men även i andra tjänster och IT-miljöer (Datainspektionen, 2017b). Vidare förväntas rätten till dataportabilitetet främja innovationsmöjligheter och uppmuntra till ökad konkurrens inom EU:s medlemsländer. Detta genom att förhindra inlåsning av medborgares uppgifter samt att se till att delning av uppgifter mellan personuppgiftsansvariga kan ske på ett säkert och enkelt sätt (Datainspektionen, 2017b).

2.1.5 Den registrerade

Inom denna studie samt i GDPRs lagtexter nämns *den registrerade*. Med den registrerade avses den fysiska person som kan knytas till de personuppgifter som behandlas (Datainspektionen, 2017f). Den registrerade har i samband med införandet av GDPR ett antal rättigheter som syftar till att ge individen information om hur och när deras personuppgifter behandlas samt att ge individen kontroll över sina uppgifter. Dessa rättigheter har i GDPR förstärkts, utökats samt specificerats i jämförelse till personuppgiftslagen (Datainspektionen, 2017f).

2.1.6 Den registrerades personuppgifter i rätten till dataportabilitet

När den registrerade väljer att utnyttja sin rätt till dataportabilitet påverkar detta ej några av den registrerades övriga rättigheter (Datainspektionen, 2017a). Den registrerade ska kunna fortsätta dra nytta och använda den personuppgiftsansvariges tjänst även efter utnyttjandet av rätten till dataportabilitet. Detta innebär alltså inte att uppgifter raderas automatiskt i enlighet med artikel 17, rätten att bli bortglömd, från den personuppgiftsansvariges system (Datainspektionen, 2017a).

I samband med rätten till dataportabilitet måste särskilda villkor uppfyllas när det gäller de personuppgifter som är aktuella och deras möjlighet till behandling och förflyttning. För det första bör de personuppgifter som är aktuella för rätten till dataportabilitet behandlats automatiskt, det vill säga att pappersuppgifter undantags. Vidare bör den insamlingen av personuppgifterna vara grundat i tidigare samtycke eller av ett avtal där den registrerade är en part av (Datainspektionen, 2017b).

För det andra bör de personuppgifter som begärs ut enbart röra den registrerade samt även tillhandahållits av den registrerade. Med "tillhandahållits av" åsyftas uppgifter som den registrerade medvetet och aktivt har bidragit till tjänsten eller IT-miljön (Datainspektionen, 2017b). Detta kan vara kontoinformation som tillhandahållits via formulär såsom e-postadress, användarnamn, ålder och kontaktlistor. Även eventuella observationer av den registrerades användning av en tjänst i IT-miljön kan anses vara uppgifter som tillhandahållits (Datainspektionen 2017a). Detta innefattar användarens aktivitet såsom aktivitetsloggar, historik, trafikuppgifter, platsuppgifter och även rådatan som behandlats av smarta mätare som t.ex. den hjärtfrekvens som mätts upp av bärbara pulsmätare.

Däremot anses inte uppgifter, information och analys som har skapats genom avledning och härledning av de uppgifter som den registrerade har tillhandahållit som uppgifter som ska omfattas av rätten till dataportabilitet (Datainspektionen, 2017a). Exempel på härleda eller avledda uppgifter som skapats av den personuppgiftsansvarige i är individanpassningsprocess, rekommendationsprocess, användarkategorisering eller profilering (Datainspektionen 2017a).

Slutligen enligt det tredje villkoret bör utövandet av rätten till dataportabilitet inte påverka rättigheter och friheter hos tredje parter på ett ogynnsamt sätt (Datainspektionen, 2017a).

Detta syftar till om en uppsättning uppgifter som överförs vid en dataportabilitetsbegäran eventuellt innehåller personuppgifter som inte enbart rör den registrerade. Då bör den nya personuppgiftsansvarige endast behandla dessa tredjepartsuppgifter om det finns en lämplig grund för sådan behandling. I de flesta fall anses endast behandling lämplig om det sker under registrerades kontroll i samband med verksamhet i ren privat natur eller som en del av den registrerades hushåll (Datainspektionen, 2017b).

2.1.7 Personuppgiftsansvarige

Personuppgiftsansvarig definieras enligt artikel 4.7 i GDPR 2016/679 av den 27 april som:

" en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter [...]"

En personuppgiftsansvarig är alltså inte en chef eller anställd på en arbetsplats, utan själva organisationen ses som personuppgiftsansvarig, med undantag för enskilda firmor där en fysisk person blir personuppgiftsansvarig (Datainspektionen, 2017d).

2.1.8 Personuppgiftsansvariges rättigheter och skyldigheter

I samband med införandet av GDPR kommer personuppgiftsansvariga ställas inför flertalet skyldigheter, en del gamla samt en del helt nya såsom dataportabilitet. Några av de skyldigheterna är inbyggt dataskydd (Privacy by Design), register över behandling, hålla en lämplig säkerhetsnivå för personuppgifter, rapportera personuppgiftsincidenter och kunna erbjuda dataportabilitet (Datainspektionen, 2017e).

En dataportabilitetsbegäran från den registrerade skall behandlas av den personuppgiftsansvarige utan onödigt dröjsmål och senast en månad efter mottagandet av begäran. Denna tidsfrist kan vid större och mer komplicerade dataportabilitetsärenden förlängas upp till tre månader (Datainspektionen, 2017a). Vid en eventuell vägran till att besvara en dataportabilitetsbegäran skall personuppgiftsansvarige informera den registrerade om orsaken till vägran samt om möjligheten att lämna in ett klagomål till Datainspektionen och begära rättslig prövning (Datainspektionen, 2017a). Personuppgiftsansvarige har även som skyldighet att utan tvivel säkerhetsställa identiteten på den registrerade som gör en dataportabilitetsbegäran genom att tillämpa ett autentiseringsförfarande. Däremot finns ofta redan dessa autentiseringsförfaranden då den personuppgiftsansvarige autentiserar användaren redan innan när den registrerade och personuppgiftsansvarige ingår avtal eller samtycke hämtas (Datainspektionen, 2017a).

Vidare är de personuppgiftsansvarige inte ansvariga för den fortsatta behandlingen av personuppgifter som sker av mottagande part vid en dataportabilitetsbegäran, oberoende om det är den registrerade själv eller ett annat företag (Datainspektionen, 2017a). Detta betyder även att en personuppgiftsansvarige ej är ansvarig för att kontrollera att den mottagande parten av en dataportabilitetsbegäran följer GDPRs föreskrifter, då en personuppgiftsansvarige ej väljer vem som ska ta emot uppgifterna (Datainspektionen, 2017a). Personuppgiftsansvarige är däremot skyldiga för att vidta lämpliga säkerhetsåtgärder som är nödvändiga för att säkerhetsställa att alla personuppgifter överförs på ett säkert sätt genom kryptering samt att datan når till rätt destination genom stark autentisering (Datainspektionen, 2017a).

I samband med mottagandet av uppgifter från en dataportabilitetsbegäran blir den mottagande organisationen en ny personuppgiftsansvarig för dessa personuppgifter. Detta innefattar de måste säkerhetsställa att de principer som anges i artikel 5 i GDPR iakttas och att den registrerades rättigheter respekteras (Datainspektionen, 2017a). En mottagande personuppgiftsansvarig har dock rättighet att neka ett mottagande och behandling av dessa uppgifter (Datainspektionen, 2017a).

En mottagande personuppgiftsansvarig är också skyldiga att kontrollera och säkerhetsställa att de uppgifter som mottages är relevanta och inte alltför omfattande för den nya uppgiftsbehandlingen. Eventuell irrelevanta uppgifter och data för den nya behandlingen bör då ej sparas eller behandlas (Datainspektionen, 2017a).

2.1.9 Formatet på personuppgifter vid en dataportabilitetsbegäran

I enlighet med rätten till dataportabilitet åläggs personuppgiftsansvariga att tillgodose att de personuppgifter som den registrerade har begärt tillhandahålls i ett format som är användbart och stöder vidareutnyttjande (Datainspektionen, 2017a). Vidare anges det mer specifikt i artikel 20.1 i GDPR 2016/679 av den 27 april som:

"i ett strukturerat, allmänt använt och maskinläsbart format".

Då det finns mängder av olika uppgiftstyper som behandlas av många olika personuppgiftsansvariga föreskriver inte GDPR några särskilda krav eller rekommendationer på formatet på personuppgifter (Datainspektionen, 2017a). Olika format är lämpligast i olika sektorer och branscher och GDPR tillsammans med Artikel-29 gruppen förordar ett starkt samarbete mellan intressenter inom samma branscher och sektorer (Datainspektionen, 2017a). Intressenterna bör tillsammans ta fram en gemensam uppsättning kompatibla format och standarder för att fullgöra de krav som rätten till dataportabilitet innebär samt uppfylla målet om tolkningsbarhet och ge registrerade hög grad av dataportabilitet (Datainspektionen, 2017a). Vidare rekommenderar Artikel-29 Gruppen att personuppgiftsansvariga utvecklar olika verktyg för att underlätta överföringen av data och rätten till dataportabilitet (Datainspektionen, 2017a). Detta kan vara tjänster och verktyg såsom API (Application Programming Interface) och webbportal för att på så sätt automatisera och effektivisera processen kring dataportabilitet (Datainspektionen, 2017a).

Om inga format har blivit standard eller allmänt använda inom en viss sektor bör öppna format användas av personuppgiftsansvariga, såsom XML, JSON och CSV (Datainspektionen, 2017a). Tillsammans bör även användbar metadata med maximal detaljrikedom och hög abstraktionsnivå ingå. Denna metadata ska användas för att på ett korrekt och fullständigt sätt beskriva betydelsen av den information som utbyts (Datainspektionen 2017a). Metadatan bör då vara tillfredsställande för att kunna använda uppgifter i dess avsedda syfte samt vidareutnyttja dem (Datainspektionen, 2017a).

2.2 Interoperabilitet

2.2.1 Introduktion

I Riktlinjer om rätten till dataportabilitet (Datainspektionen, 2017a) rekommenderar Artikel 29-gruppen verksamheter, inom samma typ av branscher eller inom samma sektor, att samarbeta för att ta fram standarder och format för att kunna möta dataportabilitetskravet från artikel 20 i GDPR. Detta innebär att verksamheter har ett behov av att uppnå interoperabilitet mellan sig (Datainspektionen, 2017a).

Problematiken kring ämnet har undersökts och diskuterats av Europeiska interportabilitetsramen (EIF) vilka kommit fram till en interoperabilitetsstrategi för organisationer som på gemensam basis vill tillhandahålla offentliga tjänster (Datainspektionen, 2017a).

2.2.2 Definitioner och syfte

Det finns åtskilliga definitioner av vad interoperabilitet betyder samt att det har olika betydelse för olika människor som alla har olika förväntningar (Chen & Daclin, 2006). Utan en gemensam vedertagen förståelse för vad interoperabilitet innebär kan man inte effektivt utveckla och spendera resurser för att uppnå den typ av interoperabilitet man önskar (Chen & Daclin, 2006). Därav har Chen & Daclin (2006) summerat olika definitioner av vad interoperabilitet egentligen betyder för att kunna bana väg för en gemensam definition. Redan 1990 definierade The Institute of Electrical and Electronics Engineers (IEEE) i sin ordbok interoperabilitet följande:

> *"Förmågan för ett eller flera system eller komponenter att utbyta information och att använda den information som har utbytts."* (IEEE, 1990)

Förenklat betyder enligt Chen & Daclin (2006) interoperabilitet följande:

1. Förmågan att dela och delge kunskap.
2. Använda sig av den delade kunskapen.
3. Gränsöverskridande funktionstillgång.

Xia & Zhao (2014) definierar interoperabilitet som en verksamhets förmåga att förvalta olikartade informationssystem med andra verksamheter. Vidare beskriver Xia & Zhao (2014) att en verksamhets informationssystem ska kunna uppnå integration och synkronisation med många olika deltagare för att räknas som interoperabilitetskompatibel. Dock påpekar Xia & Zhao (2014) att interoperabilitet är en komplex förmåga att uppnå för verksamheter då flertalet mindre förmågor först måste vara på plats. Att först kunna hantera dataflöden internt och över fasta gränser är en nödvändighet för att kunna uppnå interoperabilitet (Xia & Zhao, 2014).

Svenska forskarna Goldkuhl & Eriksson (2013) tolkar definitionen av interoperabilitet likartat med Chen & Daclin, dock med fokus på elektronisk förvaltning som deras studie handlar om. En tydlig definition av interoperabilitet anser Cimander, Kubicek & Scholl (2011) som viktigt då många intressenter ofta tror att interoperabilitet uppnås med hjälp av internet, när det endast tillhandahåller interoperabilitet i form av dirigering och transport av bits. Det intressen-

terna ofta glömmer är vikten av den ömsesidiga förståelsen för den delade datan och hur koordineringen av olika arbetsflöden bland verksamheter ska gå till för att uppnå interoperabilitet (Cimander et. al, 2011). Enligt Allen, Karanasios & Norman (2014) är det av högsta relevans att inte bara se interoperabilitet som ett problem vars lösning är av teknisk natur. Att uppnå interoperabilitet är mer en fråga som kräver förvaltning på ett organisatoriskt och informativt vis, då det är mer styrt av inbördes normer och värderingar (Allen et al, 2014).

2.2.3 Barriärer

För att kunna förstå interoperabilitet är det fundamentalt att känna till interoperabilitetsbarriärer (Chen & Daclin, 2006). Dessa barriärer är vad Chen & Daclin (2006) menar som inkompatibilitet mellan olika systems förmågor att utbyta information. Uppdelningen av barriärer är konceptuella, tekniska och organisatoriska barriärer (Chen & Daclin, 2006). Med den konceptuella barriären avser Chen & Daclin (2006) semantisk och syntaktisk interoperabilitet.

Den syntaktiska problematiken uppstår genom att olika människor och olika system använder olika strukturer för att representera information (Chen & Daclin, 2006). Den semantiska problematiken grundar sig i att information och kunskap representeras på olika sätt i olika modeller eller mjukvara, samt att det inte finns någon entydig och klardefinierad betydelse för informationen (Chen & Daclin, 2006). Denna problematik försöker lösas genom ontologistudier, vilket är läran om verkligheten (Chen & Daclin, 2006).

Den tekniska barriären är förankrad i avsaknaden av kompatibla standarder för hur verksamheter ska kunna kommunicera och dela information över heterogena tekniker mellan två eller flera system (Chen & Daclin, 2006). Denna problematik grundar sig i att verksamheters IT-arkitektur, infrastruktur, operativsystem ser olika ut beroende på vilken sektor man arbetar i (Chen & Daclin, 2006). Ett par konkreta exempel på tekniska barriärer kan vara användningen av olika kommunikationsprotokoll för informationsdelning, olika metoder för att presentera information samt olika tekniker för att tolka delad information (Chen & Daclin, 2006). Även om det redan finns etablerade tekniska standarder inom ett visst område, så existerar barriären med att olika versioner av samma standard används samtidigt (Chen & Daclin, 2006). Allen et al (2014) menar också att filosofin kring hur man utvecklar system idag inte främjar interoperabilitet.

Chen & Daclin (2006) presenterar den sista barriären inom interoperabilitet som organisatorisk. Inkompatibiliteten i organisationsstruktur, verksamhetsförvaltning och förvaltningstekniker mellan två eller flera verksamheter försvårar interoperabiliteten (Chen & Daclin, 2006). Cimander et. al (2011) förstärker detta genom att påpeka den organisatoriska interoperabilitetens problematik genom den obefintliga koordineringen, oreglerade arbetsflöden och komplexa auktoritetsstrukturer mellan olika verksamheter. Konkreta exempel på organisatoriska barriärer kan vara att ansvarsuppdelning är odefinierad mellan involverade parter, även otydligt definierad behörighet av vem som får göra vad, samt olika organisatoriska strukturer (Chen & Daclin, 2006).

2.3 Privacy by Design

Begreppet Privacy by Design innebär i grunden att från ett så tidigt stadie som möjligt ska personlig integritet inbäddas i systemutveckling, processer, verksamheters infrastruktur och nätverk (Cavoukian, 2012). Syftet enligt Cavoukian, är att använda Privacy by Design som strategi där fokus måste ligga på att göra den personliga integriteten till en kärnfunktion via strategisk ledning och genomtänkt ingenjörskonst (Cavoukian, 2012). Privacy by Design kan också ses som ett ramverk för hur problematiken med att översätta sociala, etiska och legala krav ska lösas till en reell verklighet (Diaz, et al 2011). Därav ska man inte anamma Privacy by Design som endast organisationspraxis att följa i förändringssyfte för att möta integritetskrav, utan även i rent tekniskt och designmässigt syfte (Cavoukian, 2012). Projektledare och systemarkitekter borde därför försöka producera genomtänkta säkerhetsåtgärder för att behandla problem som ligger i nutiden, men åtgärderna ska också försöka bygga för att handskas med framtida problem (Schaar, 2010).

Vad detta mer konkret betyder kan summeras i att verksamheter som behandlar personlig information ska försöka att anamma dataminimering, vilket betyder att man ska försöka samla, behandla och spara så lite personlig data som möjligt (Diaz, et al 2011). Detta innebär också att anonymisering och radering ska finnas tillgänglig och brukas på nödvändigaste sätt för att främja integriteten (Schaar, 2010). Det är viktigt att påpeka att integritet ska byggas in i själva systemarkitekturen och ska has i åtanke från start till slut i bygget av ett IT-system, från ritbordet till implementationsfasen (Schaar, 2010).

Privacy by Design anses också vara en typ av måttstock på att hantera oklarheten som finns i sekretesslagstiftningar genom att underlätta medvetenhet kring integritet även i miljöer där mycket data hanteras (Everson, 2017).

Cavoukian (2012) menar på att Privacy by Design går att uppnå genom att försöka anamma och efterleva 7 stycken fundamentala principer. Dessa principer är, som nämns i första principen proaktiva, och borde inte användas av verksamheter i reaktivt syfte på uppdagat problem utan som strategi på en högre konceptuell nivå i förebyggande syfte.

1. **Proactive not reactive; Preventative not remedial.**

   Den första fundamentala principen av Cavoukian (2012) menar på att Privacy by Design är proaktiv istället för reaktiv i sina åtgärder. Genom att implementera strategier och metoder för att undvika sekretessöverträdelser innan de sker i en tidig designfas av ett informationssystem, så kan inte riskerna förverkligas (Cavoukian, 2012). Vidare påpekas vikten av att förstå att Privacy by the design inte ger svar på varför en unik överträdelse skett, utan fokus ligger på förebyggande (Cavoukian, 2012).

2. **Privacy as the Default Setting**

   Ett av huvudmålen med Privacy by Design är att kunna leverera högsta möjliga integritetsskydd genom att personuppgifter automatiskt säkras via tekniska och organisatoriska processer (Cavoukian, 2012). Det ska inte krävas interaktion av varken den registrerade eller personuppgiftsansvarige för att personuppgifterna ska vara säkra i systemet. Identitetsskydd ska finnas inbyggt i systemets arkitektur som standard (Cavoukian, 2012).

3. Privacy Embedded into Design

Tredje principen stadgar att integritetsskydd ska vara invävd i designen och arkitekturen av IT-systemet och verksamheten och inte vara beroende av något tilläggsprogram eller kompetent som tillförs i efterhand. Genom att integrerar detta från början minskar man problem med sekretessen utan att rubba funktionaliteten (Cavoukian, 2012).

4. Full functionality

Privacy by Design har som utgångspunkt att de föreställda dikotomierna såsom att ta ett speciellt val utan konsekvens är felaktiga. Detta innebär att via Privacy by Design behövs inte integritet ställas mot säkerhet, vilket exempelvis innebär att implementera integritetsskydd i sina IT-system/verksamhetsprocesser och att samtidigt få till fullskaligt skydd. Att istället ha som mål att alltid uppnå full funktionalitet i ett ömsesidigt "win-win"-scenario, är det som Privacy by Design ämnar att avse (Cavoukian, 2012).

5. End-to-End Security - Full lifecycle Protection

Att väva in Privacy by Designs fokus på integritetsskydd redan från start i verksamheters system- och verksamhetsarkitektur, ska datan som insamlas vara skyddad under hela livscykeln. Detta betyder säkerhet från insamlandet av datan tills att den raderas i enlighet med satt tidsram (Cavoukian, 2012).

6. Visibility and Transparency - Keep it Open

Privacy by Design ämnar att samtliga personuppgiftsansvariga ska kunna försäkra och införliva förtroende till samtliga intressenter, att de riktlinjer och avtal som upprättats verkligen följs. Om den personuppgiftsansvarige vidhåller en genomgående transparens till sina intressenter (registrerade och leverantörer) så kan förtroende mellan parterna säkerställas och förvaltas (Cavoukian, 2012).

7. Respect for User Privacy - Keep it User-Centric

Privacy by Design förespråkar att personuppgiftsansvariga ska försöka vidhålla sina intressenters intressen som sin största prioritering. Detta kan erbjudas genom kraftiga åtgärder mot bättre integritetsvillkor, stark uppföljning och verifikation av riktlinjer och avtal samt att arbeta mot en mer användarcentrerad miljö. Det viktiga är att alltid sätta intressenten i fokus (Cavoukian, 2012).

2.4 Tekniska verktyg och format

2.4.1 API

Application programming interface, eller API, tillhandahåller användare en problemgeneralisering samt hur användaren specifikt ska interagera med mjukvarukomponenter som löser det generaliserade problemet (Reddy, 2011). Dessa komponenter är ofta distribuerade via mjukvarubibliotek, vilket gör att dessa tillåter användaren att använda dessa i många olika applikationer. API:er definieras av återanvändbarhet genom byggstenar som tillåter modulära bitar av funktionalitet vars syfte är att införlivas i olika slutanvändarapplikationer (Reddy, 2011). API:er skapas till dig själv, andra yrkespersoner i din organisation eller i syfte att främja utvecklingen för en bredare publik via olika intressegrupper. Innehållet i ett API kan variera avsevärt. Det kan variera från att bestå av en enda funktion till hundratals klasser, metoder, datatyper och konstanter. Huvudsakligen är API:er ett väldefinierat och tydligt gränssnitt som erbjuder specifika tjänster till olika mjukvaror (Reddy, 2011).

2.4.2 XML

Extensible Markup Language, eller XML, är ett datalagringsverktyg samt en konfigurerbar farkost för all typ av olik information (Ray, 2003). XML är både ett protokoll för innehåll och förvaltning av information, men är lika mycket teknik som kan formatera dokument eller filtrera data (Ray, 2003). XML kan också ses som en filosofi inom informationshantering vars mål är att maximera användbarheten och flexibiliteten för data genom raffinering till en strukturerad form (Ray, 2003). Nedan följer enligt Ray (2003) några konkreta funktioner som XML har:

1. Då XML är open source äger inget företag det och det kräver ingen speciell mjukvara för att användas.
2. Kvalitetskontroll genom syntaxregler, intern länkkontroll, jämförelser av dokumentmodeller och programmeringsspråk.
3. Simpel och entydig syntax och struktur vilket gör det lättläst och lättanalyserat för människor såväl som datorsystem.
4. Stöd för ett stort antal skrivsystem och symboler.

2.4.3 CSV

A Comma Separated Value, eller CSV, har används under lång tid för spara, dela och konvertera data och text i tabellformat (Shafranovich, 2005). CSV-filer är lika XLSX-filerna som många känner igen från användning av Microsoft Excel vilket är ett program för elektroniska kalkyler. Skillnaden från en XLSX-fil är att CSV-filen är att varje datarad representerar en post och varje post representerar en eller flera fält som separerar via kommatecken. Detta kommatecken används för att separera olika typer av data (Shafranovich, 2005).

2.5 Verksamhetsförändringar

2.5.1 Business Process Management

En process definieras enligt Harmon (2014) som en sammanhängande grupp av aktiviteter som utförs som svar till en inledande händelse för att i sin tur generera ett värdefullt resultat. Processer kan vara både väldigt enkla eller extremt komplexa (Harmon, 2014). Ett annat viktigt koncept enligt Harmon (2014) är processhierarkier, att använda sig av nivåer för att beskriva hierarkierna. Dessa hierarkier kan generaliseras till tre olika nivåer; hög-, medium- och lågnivå. Utifrån nivåerna kan man sedan knyta olika slags problem samt analystekniker lämpliga för varje enskild nivå (Harmon, 2014).

2.5.2 Processhierarkier

Den högsta nivån syftar oftast till arkitekturella problem inom verksamheten. Analysen på denna nivå bör undersöka de största verksamhetsprocesserna, deras input, output och mätetal (Harmon, 2014). Problem som kan identifieras kan vara sådana som berör koordineringen mellan olika avdelningar eller enheter (Harmon, 2014). På denna nivå menar Harmon (2014) att fokus bör ligga på att se till att input ligger i linje med output samt att skapa kontrakt för vad process A behöver leverera till process B.

På mellannivån bör enligt Harmon (2014) fokus av analysen ligga på de processer som är en del av de största verksamhetsprocesserna samt deras subprocesser. Problem på mellannivån kan uppstå i processer som hanteras eller sker inom en eller ett par avdelningar (Harmon, 2014). Problemen kan kräva att processer förenklas eller dess ordningsföljd ställs om. Samtidigt bör processer som inte adderar värde tas bort och några aktiviteter kan behövas bli automatiserade (Harmon, 2014).

Vidare menar Harmon (2014) att problem som finns på den lägsta nivån oftast syftar till enskilda individers prestation eller de mjukvarusystem som används. Här bör en analys ske på en detaljerad nivå kring varje aktivitet med fokus på procedurens steg, de olika rollerna, regler som finns och de olika informationssystemen som används (Harmon, 2014). I vissa fall behöver vissa styrdokument eller informationssystemen specificeras eller rättas till. Träningsprogram eller arbetsbeskrivningar kan ofta behöva utvecklas (Harmon, 2014).

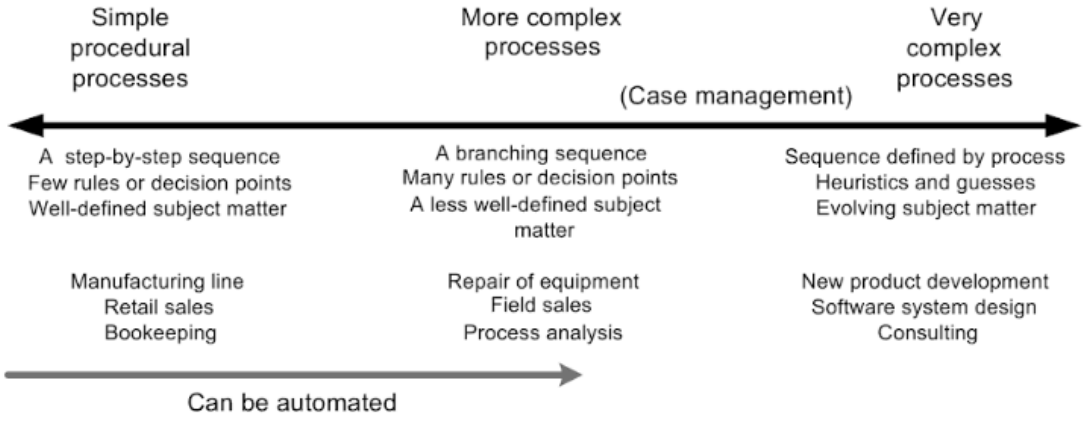
2.5.3 Enkla och komplexa processer

Ett annat sätt att analysera och förändra processer enligt Harmon (2014) är som nämnt tidigare att dela upp processer i olika komplexitetsgrad. Utifrån processernas identifierade komplexitetsgrad kan man sedan avgöra lämpliga åtgärder och förändringar samt undersöka om de är lämpliga att bli automatiserade (Harmon, 2014).

Vad Harmon (2014) kallar enkla processer är de processer som följer en konsekvent och väldefinierad sekvens av steg med klara regler. Varje aktivitet kan här bli tydligt preciserad och dess sekvens saknar avgreningar eller olika undantag (Harmon, 2014). En lite mer komplex

process kännetecknas enligt Harmon (2014) av avgreningar och olika undantag i dess sekvens. Här finns många regler att ta hänsyn till och processens aktiviteter tenderar att vara mindre väldefinierade. Dessa processer kräver mer initiativ och inverkan av mänskliga medarbetare (Harmon, 2014). Vidare menar Harmon (2014) att väldigt komplexa processer kräver ännu mer initiativ och kreativitet från mänskliga medarbetare. Dessa processer kan normalt sett inte bli automatiserade med dagens teknologi samt att man vanligtvis inte kan utbilda medarbetare att genomföra dessa uppgifter (Harmon, 2014). Istället anställs människor med högre utbildning och erfarenhet som besitter de kreativa och analytiska förmågorna som krävs för att utföra uppgifter (Harmon, 2014). Dessa processer är ännu mindre definierade, ändras ofta och utvecklas under tiden (Harmon, 2014).

Vidare presenterar Harmon (2014) ett spektrum som förklarar hur processer har olika komplexitetsgrad, exempel på uppgifter för varje grad samt vilka av dessa som är lämpliga för automatisering.



Figur 2.1: The process continuum (Harmon, 2014)

2.5.4 Förändringsarbete ur ett ledarperspektiv

Förändringsarbete definieras enligt Moran & Brightman (2000) som en process av ett kontinuerligt förnyande av en verksamhets riktning, förmågor, kompetens och struktur. Detta för att ligga i linje med de ständigt förändrade behoven av externa och interna intressenter. Behovet av förändring är enligt Todnem By (2005) ofta oförutsägbart. Förändringsbehovet tenderar att vara reaktivt, osammanhängande och framprovocerat av en organisatorisk kris (Todnem By, 2005). Moran och Brightman (2000) menar även att förändringsarbete är icke-linjärt där inget tydligt definierad start eller slut finns på förändringen utan att den sker cykliskt.

Todnem By (2005) menar att det är svårt att hitta konsensus för ett enskilt ramverk som ska appliceras vid förändringsarbete och att många olika alternativ finns. Moran & Brightman (2000) presenterar utifrån sin idé om att förändringar sker cykliskt sitt egna ramverk The change management cycle och det innehåller fyra olika faser som ska itereras:

1. **Förstå den nuvarande situationen:** Vid förändringsarbete krävs det att förändringsledaren kan se den större bilden. Att man kan se förändring i kontext av vad som sker i sin omgivning. Detta kan vara förändringar såsom förändrade kundbehov, nya konkurrenter, teknologier eller förändringar inom det statliga, legala eller ekonomiska klimatet (Moran & Brightman (2000). Förståelse av hur dessa externa förhållanden kommer påverka verksamheten kommer vara en stark anledning och hjälp vid organisationsförändring (Moran & Brightman, 2000). Vidare menar Moran & Brightman (2000) att en förändringsledare även måste se situationen från den lokala nivån såsom den globala nivån. Detta genom att samtala och förstå de människor och processer som är delaktiga och kommer påverkas av förändringen. Förändringsledaren måste utveckla en uppskattning för deras synvinkel och även förstå varför de människorna ser det på det sättet de gör (Moran & Brightman, 2000).

2. **Bestämma det önskade tillståndet och utveckla en förändringsplan:** Nästa fas i cykeln menar Moran & Brightman (2000) är att ta lärdom från både den globala nivån och lokala nivån för att utveckla en sammanhängande plan. Till en början brukar det vara meningsskiljaktigheter kring hur förändringen ska se ut och genomföras. Det är då förändringsledarens uppgift att analysera och sätta ihop de olika perspektiven till ett konkret mål som tilltalar många (Moran & Brightman, 2000). Visionen ska sedan presenteras i klara och konkreta termer som alla kan förstå. Samtidigt bör en plan skapas som stegvis förklarar hur förändringen bör genomföras och uppfyllas (Moran & Brightman, 2000).

3. **Få med andra och nå en kritisk massa:** Tredje fasen i cykeln menar Moran & Brightman (2000) är att etablera förändringen i verksamheten. Att implementera breda organisatoriska förändringar kräver flertalet kommunikationsfärdigheter och en djup nivå av kunskap som enbart en person ej kan besitta (Moran & Brightman, 2000). Förändringsledaren kommer behöva hjälp av andra i organisationen. Att implementera en förändring bör alltid innehålla en testperiod menar Moran & Brightman (2000). Flertalet förhållningssätt och strategier kan behöva testas innan förändringsarbetet ger resultat och vid denna period krävs människor som är villiga att testa olika idéer och tillvägagångssätt och som då samtidigt inte blir avskräckta av initiala misslyckanden. Emellertid om en förändringsledare skulle lyckas genomföra en förändring själv så kommer medarbetarnas hjälp behövas för att upprätthålla förändringen inom organisationen (Moran & Brightman, 2000). Moran & Brightman (2000) menar att som förändringsledare bör man kontinuerligt involvera mer och mer människor i förändringen och förändringsarbetet för bygga en brett stöd för förändringen i organisationen. Alltså, nå en så kallad kritisk massa av stöd och på så sätt säkerhetsställa förändringen och dess acceptans i verksamheten. Om detta ej säkerhetsställs så finns det risk för att förändringen återgår till tidigare stadie (Moran & Brightman, 2000).

4. **Spåra och stabilisera resultat:** Den fjärde och sista fasen menar Moran & Brightman (2000) är att följa upp och stabilisera resultat som ligger till följd av förändringen. Detta bör ske genom att förändringsledaren sätter upp prestationsmål och mätetal. Genom att kontinuerligt mäta och följa upp resultat som ligger till följd av förändringsarbetet ges insikt kring hur verksamheten förhåller sig till de utsatta målen (Moran & Brightman, 2000).

2.6 Undersökningsmodell

Modellen nedan är framtagen och baserad på litteraturgenomgången, utifrån vilken vi sammanställt relevanta kategorier med centrala begrepp i syfte att kunna utföra undersökningen. Undersökningsmodellen är ämnad till skapandet av intervjufrågor samt säkerställandet att dessa frågor har relevans för syftet med undersökningen.

Tabell 2.1: Undersökningsmodell

Kategori	Litteratur	Undersöker
GDPR - Dataportabilitet	**GDPR** (Datainspektionen, 2017i), (Datainspektionen, 2017h) **Personuppgifter** (Datainspektionen, 2017c), (Datainspektionen, 2017g) **Dataportabilitet och dess syfte** (Dataportabilitet, 2017a), (Datainspektionen, 2017b) **Den registrerade** (Datainspektionen, 2017a), (Datainspektionen, 2017b), (Datainspektionen, 2017f) **Den personuppgiftsansvarige** (Datainspektionen, 2017d) **Dataportabilitetsbegäran och dess format** (Datainspektionen, 2017a)	Definitionen av personuppgift Den registrerades uppgifter Personuppgiftsbehandling Rätten till dataportabilitet Åtgärder för tillmötesgående
Interoperabilitet	**Definitioner av Interoperabilitet** (Datainspektionen, 2017a), (Chen & Daclin, 2006), (Xia & Zhao, 2014), (Goldkuhl & Eriksson, 2013), (Allen et al, 2014), (Cimander et. al, 2011), (IEEE, 1990) **Syntaktiskt & semantisk barriärer** (Chen & Daclin, 2006) **Teknisk barriärer** (Chen & Daclin, 2006), (Allen et al, 2014) **Organisatorisk barriärer** (Chen & Daclin, 2006), (Cimander et. al, 2011)	Tekniskt branschsamarbete Organisatoriskt branschsamarbete Standardformat
Privacy by Design	**Minimering av datahantering** (Diaz, et al 2011), (Cavoukian, 2012) **Anonymisering & radering** (Schaar, 2010), (Cavoukian, 2012) **Inbyggd säkerhet** (Cavoukian, 2012), (Schaar, 2010)	Användandet av Privacy by Design vid verksamhetsförändringar Privacy by Design som strategi

	Privacy by Design som strategi och tankesätt (Cavoukian, 2012), (Everson, 2017)	
Tekniska verktyg och format	**API** (Reddy, 2011) **XML** (Ray, 2003) **CSV** (Shafranovich, 2005)	Upprättandet av ett API Tänkta format vid dataportabilitets-begäran
Verksamhets-förändringar	**Processförändringar** (Harmon, 2014) **Processhierakier** (Harmon, 2014) **Processkomplexitet och möjlighet till automatisering** (Harmon, 2014) **Förändringsarbete ur ett ledarperspektiv** (Moran & Brightman, 2000), (Todnem By, 2005) **Change management cycle** (Moran & Brightman, 2000)	Åtgärder i form av nya processer Organisationsförändringar Automatisering av processer

3 Metod

I detta kapitel kommer valet av tillvägagångssätt och vilken vald vetenskaplig metod presenteras, vilka användes för att besvara frågeställningen. Vidare presenteras hur den kvalitativa studien genomförts samt hur databearbetning och analys utförts. Ytterligare ges en genomgång av hur undersökningskvaliteten legat till grund för hur vi utformat vår studie i syfte att minimera felmarginaler och höja kvaliteten på studien.

3.1 Insamling av Empirisk data

3.1.1 Metodval

Vid insamlandet av empirisk forskningsdata brukar man använda sig av två olika metodologier. Dessa två är antingen kvantitativ eller kvalitativ studie (Jacobsen, 2002). Vid utförandet av en kvalitativ studie brukar forskningsdata samlas in från ett antal informanter. Fördelen med samla in forskningsdata via kvalitativa intervjuer är djupet och kvalitén på data som dessa intervjuer medför, då mer utförliga svar kan ges till problem eller frågor (Jacobsen, 2002). Om man även försöker ha en öppen och avslappnad dialog mellan den undersökande och informanten, utan för strikt och förutbestämt frågematerial kan ytterligare djup av forskningsdata hittas (Jacobsen, 2002). Vid en kvantitativ studie blir dock analysen av data något mer generaliserad då ansatsen är ett mycket större antal informanter där det ofta finns fördefinierade svarsalternativ. Jacobsen (2002) menar att detta gör insamlad data mindre detaljerad då informanterna inte fått möjlighet att motivera varför de valt ett visst svarsalternativ (Jacobsen, 2002).

I vår studie har vi därför fokuserat på att få så utförliga och djupa svar som möjligt, och därför utfört en kvalitativ studie. Detta för att kunna få en bredare bild kring olika typer av verksamheters utmaningar med att lösa dataportabilitetsbegäran samt vilka förändringar som skett med detta krav. Jacobsen (2002) menar att en bra metod är djupgående intervjuer med personer som är insatta i forskningsområdet och områdets bakgrund. Därför har vi med omsorg valt vilka verksamhetsrepresentanter som borde vara relevanta för att skapa en detaljerad bild av problematiken i praktiken. Dessa personer har i regel fått samma frågor som finns sammanställda i appendix. Responsen från informanterna har resulterat i att vi ibland ställt följdfrågor, dessa har dock hög relevans för att öka detaljrikedomen i det som informanterna beskrivit. Intervjufrågorna är sammanställda utifrån vår undersökningsmodell som är uppbyggd av vår litteraturgenomgång. Därför är dessa frågor relevanta för att besvara vår frågeställning. Vi har också begränsat oss till fem grundliga intervjuer då tidsbrist varit det största problemet.

3.1.2 Urval

Vid urvalsprocessen jobbade vi med att försöka säkerställa korrektheten och kvaliteten men också att intervjuerna skulle fortlöpa smidigt och kravlöst. Vi arbetade fram urvalet av informanterna i kvalitetssyfte utifrån vår frågeställning, vilket anses av Jacobsen (2002) fördelaktigt. Vår avsikt med urvalet var att hitta informanter med relevant erfarenhet av GDPR- och dataportabilitetsfrågor. Den erfarenhet vi sökt hos informanterna är att vederbörande ska ha

jobbat med något tekniskt, organisatoriskt, processorienterat eller säkerhetsmässigt perspektiv kring GDPR, dataportabilitet och förändringsarbete mot tillmötesgående. Dock var verksamhetsurvalet relativt öppet då samtliga verksamheter ska kunna erbjuda dataportabilitet om de hanterar personuppgifter. Detta gjorde att vi kunde fokusera på flera sektorer och bredda vår sökning efter informanter.

Informanterna som vi slutligen intervjuade hade alla olika yrkesroller och erfarenhet. En informant jobbade inom projektledning och en annan jobbade som informationssäkerhetschef, men samtliga hade yrkesroller, och jobbade inom sektorer, relaterade till arbete med GDPR och dataportabilitet. De olika rollerna hos informanterna gav oss en mer överskådlig bild över problemet vi vill undersöka. Vi ville inte rikta in oss enbart på en specifik sektor eller yrkesroll då informantens åsikter kunnat vara alldeles för färgade av verksamheten vederbörande arbetar i. Detta hade möjligen gett oss en för snäv bild över det övergripande problemet.

Inledningsvis kontaktades de verksamheter vi först tänkt oss som potentiella informanter via e-post, dock var responsen inte helt optimal och ytterligare övertalning fick ske via telefon. I mailen och via telefon presenterade vi oss själva samt syftet med studien och frågade om vi kunde få komma i kontakt med någon inom verksamheten som hade kunskap och erfarenhet inom området. Vederbörande vidarebefordrade oss efter våra önskemål till en person som de ämnade vara rätt person att svara på våra frågor. Därefter resulterade mailkorrespondensen eller telefonsamtalet med en inbokad intervju eller diverse avböjande. Några verksamheters avböjande berodde på otillräckligt med tid, okunskap i området eller sviktande intresse att vara med i vår studie. Slutligen fick vi utfört fem stycken djupintervjuer med en diversifierad informantskara.

3.1.3 Informanter

Tabellen presenterar samtliga informanter där två är pseudonymiserade enligt önskemål. Även presenteras informantens verksamhet, roll i verksamheten, var intervjun hölls och dess längd. Samtliga intervjuer hölls på plats hos verksamheterna och finns att läsas under appendix.

Tabell 3.2: Informanter

Informant	Namn	Företag	Roll	Plats	Längd
IF1	Informant 1	Företag A (Bank)	IT-chef	Helsingborg	28:43
IF2	Magnus Persson	LDC	IT-säkerhetsarkitekt	Lund	54:10
IF3	Informant 3	Företag B (Elbolag)	Information Security Manager	Malmö	41:36
IF4	Christer Björmander	Skånetrafiken	IT Förvaltningsledare	Lund	58:02
IF5	Johannes Sporre	Kraftringen Energi AB	Projektledare GDPR	Lund	45:07

3.1.4 Uppförande av intervjuguide

Då dataportabilitet är komplext och bidrar till olika utmaningar beroende på vilken verksamhet och vilken sektor verksamheten opererar inom, kommer informanterna ge vitt skilda svar. I syfte att minimera analysarbetet som annars kunnat bli väldigt omfattande så utformade vi vår intervjuguide efter vår undersökningsmodell. Intervjuguidens syfte är att lyfta och belysa olika teman som är relevanta för vår studie. Våra intervjuer utfördes med hjälp av intervjuguiden som vi konstruerade med en semistrukturerad frågestruktur, något som Jacobsen (2002) förespråkar för att inte göra intervjun för sluten. Vi gav inga fördefinierade svarsalternativ vilket gav vederbörande möjlighet att prata öppet kring våra frågor. Vi utformade också intervjun så att vi hade möjlighet att ställa relevanta följdfrågor till informanten. Detta gjorde vi för att kunna få ut extra information och eventuellt belysa ytterligare aspekter av en fråga.

3.1.5 Genomförande av intervjuerna

Avsikten för intervjugenomförandet var att hålla fysiska intervjuer där informanten befann sig i samma rum som undersökaren. Det vi ämnade uppnå vid en fysisk intervju var att få detaljrikedom och nyanserade utläggningar i svaret från informanten (Jacobsen, 2002). Vidare skriver Jacobsen (2002) att vid fysiska intervjuer är det svårare för informanten att ljuga då man är i samma rum som undersökaren. Om man däremot håller en intervju över telefon går en viktig dimension förlorad i frånvaron av ansiktsuttryck och kroppsspråk (Jacobsen, 2002). Att försäkra informanten om anonymisering kan vara ett sätt att minska påverkningen från det som Jacobsen (2002) kallar för intervjueffekten. Vid ett fysiskt möte kan det uppfattas svårt att tala öppet till skillnad från vad det hade gjort vid ett anonymiserat samtal över telefonen, detta på grund av effekten som undersökaren kan ha på informanten (Jacobsen, 2002).

Våra intervjuer inleddes med att vi frågade informanten om det gick bra att vi spelade in intervjun. Detta gjorde vi för att säkerställa att ingen information gick till spillo då vi hade för avsikt att transkribera intervjun och analysera materialet. Jacobsen (2002) förespråkar inspelade intervjuer just i syfte att kunna gå tillbaka för senare analys. Vår önskan var även att få informanten att tala avslappnat utan att behöva stoppa informanten mellan utläggningar och frågor, vilket kunnat ske i stor utsträckning om vi antecknat istället för spela in. Därefter förklarades att informanten hade rätt till att vara anonym om hen önskade, och att vi endast hade för avsikt att i så fall nämna vilken bransch och roll vederbörande verkar i. Vidare följde vår intervju en tematisk modell med frågor som först behandlade vilken roll, erfarenhet och akademisk bakgrund informanten hade.

Därefter var upplägget av frågorna mer övergripande kring dataportabilitet för att sedan gå över till tekniska utmaningar, process- och organisatoriska utmaningar. I intervjuns slutskede ställdes frågor till informanten kring strategin och ramverket Privacy by Design och om detta används för att utveckla nya processer eller tekniska lösningar för att erbjuda dataportabilitet. Frågorna formulerades inte exakt enligt de fördefinierade frågorna i intervjuguiden, men väldigt snarlikt och med samma syfte. Om vi ansåg att informanten gav svar till flera frågor i ett och samma svar, ställde vi inte frågan som vi ansåg besvarad på nytt. Detta för att försöka minska upprepning och hålla intervjuerna innanför någorlunda tidsram. Avslutningsvis gav vi informanten möjlighet att försöka sammanfatta vad hen ansåg vara den övergripande största utmaningen med att kunna erbjuda dataportabilitet.

3.2 Bearbetning av data

Jacobsen (2002) påpekar relevansen i att strukturera sitt empiriska material i form av kategoriseringen och systematisering vid analysprocessen. Då vi transkriberade samtliga intervjuer i sin helhet ger detta en tydlig översikt över forskningsdata. Vi valde dock att sålla bort otydligheter som uppstod. Dessa kunde vara moment som otydligt tal eller om relevansen frångicks (Jacobsen, 2002). I transkriptionen har vi även gjort bitar läsbara genom att strukturera texten så att den frångår talspråk till läsligt skriftspråk. Detta är gjort för att underlätta för läsaren att förstå vad informanten menar. Vid samtliga intervjuer frågade vi informanten om vederbörande önskade vara anonym vilket enligt Jacobsen (2002) är en trygghetsfaktor för informanten. Vi har vidare på begäran fått pseudonymisera två informanter vilket förtydligas under informanter. I analysprocessen jämförde och sammanställde vi informanternas svar i tabellform som presenteras under resultat. Vi valde också att strukturera upp det empiriska resultatet med fokus på de viktigaste förutbestämda frågorna samt följdfrågorna för forskningsområdet. Detta är ett aktivt val för att konkretisera empirin och göra det avsevärt lättare för läsaren. I transkriptionen har samtliga svar och frågor numreras för att underlätta arbetet med att referera i vidare analysarbete. Detta är också avsett för att läsaren ska kunna hitta var i empirin följande svar hämtats ifrån.

3.3 Undersökningens kvalitet

För att försöka hålla undersökningskvaliteten så hög som möjligt ämnade vi att hålla undersökningarna så lika så möjligt i sin natur. Målet var att påverka informanten till den lägsta möjliga grad. Därav skickade vi ut förfrågningar i syfte att tydligt och strukturerat informera vad vi ämnade undersöka och på vilka villkor intervjuer skulle ske. För att kunna utvärdera kvaliteten i vår undersökning måste den granskas och detta har gjorts genom en validitets- och reliabilitetsanalys (Jacobsen, 2002).

3.3.1 Validitet och reliabilitet

Jacobsen (2002) förespråkar att den insamlade empiriska forskningsdatan ställs inför två krav. Dessa krav är validitet och reliabilitet (Jacobsen 2002). Forskningsdatan ska vara giltig och relevant samt att den måste vara tillförlitlig (Jacobsen, 2002). Jacobsen (2002) delar upp validiteten i intern och extern validitet, där den interna validiteten syftar på hur trovärdig forskningsdatan är medan den externa syftar på hur väl resultaten av empirin kan generaliseras (Jacobsen, 2002).

För att stärka studiens interna validitet var intervjuerna av samma struktur i syfte att ge samtliga informanter likartade förutsättningar. Vidare erbjöd vi samtliga informanter kopia av transkriberingen för att vederbörande skulle kunna korrigera eller ta bort svar som denne i efterhand ansåg felaktiga eller opassande. Då undersökningen är baserad på litteraturgenomgången stärks den interna validiteten ytterligare, detta genom att intervjuguiden bygger på vår undersökningsmodell. I syfte att stärka den externa validiteten av vår studie hade alla informanter arbetsroller inom sfären för vårt forskningsområde och innehar kunskap om vårt berörda problem.

Vår undersöknings tillförlitlighet (reliabilitet) förstärktes då vi arbetade mot att minimera det som Jacobsen (2002) kallar för kontexteffekt. Effekten beror på om undersökningen sker på en plats som är okänd för informanten eller om undersökningen varit planerad eller inte (Jacobsen, 2002). Då vi i förväg planerat intervju med informanten, vilket gett tid till vederbörande att förbereda sig, samt bokat in på vilken plats intervjun skulle ske, motverkade vi denna effekt. Jacobsen (2002) beskriver också intervjueffekten där informanten på något sätt färgas av undersökaren via olika typer av intryck. Då vi förde våra intervjuer fysiskt på plats påverkade vi informanten, vilket kan ses som oundvikligt.

3.3.2 Kritik mot tillvägagångssätt

Då vi utförde vår undersökning via semistrukturerade intervjuer ställde vi följdfrågor där vi ansåg att informanten inte svarade tillräckligt utförligt. Dessa följdfrågor kan ses som ledande och måste därför tolkas på ett mer varsamt sätt. Vidare utfördes litteraturstudien innan undersökningen vilket kan ha färgat vad vi anser vara rätt eller fel. Även vår undersöknings storlek kan göra resultatet svårt att generalisera, då fler informanter eventuellt behövts (Jacobsen, 2002). För att hantera de ofta väldigt detaljerade svaren använde vi oss av en strukturerad kategorisering och numrering vid presentationen av resultatet.

3.3.3 Etik

Under genomförandet av undersökningen har det funnits olika etiska aspekter att förhålla sig till. För att undvika att etiska dilemman uppstår vid en undersökning menar Jacobsen (2002) att tre grundkrav bör uppfyllas. De olika kraven Jacobsen (2002) fastslår är: Informerat samtycke, krav på privatliv och krav på att bli korrekt återgiven. Informerat samtycke innebär att informanten med fullständigt samtycke medverkar i studien, förstår syftet med den empiriska studien och på vilka villkor undersökningen kommer utföras (Jacobsen, 2002). Vid utskick av förfrågningar om informanter till verksamheter informerade vi tydligt vårt syfte med studien, hur vi tänkt genomföra den, samt ställde frågan om vem som verksamheten själv rekommenderade att vi skulle tala med. Förfrågan förklarade även att informanten och verksamheten hade rätt till fullständigt anonymisering som så önskades. Därigenom fick samtliga informanter fullständigt klarhet i vad vår förfrågan medförde och accepterade detta helt frivilligt. Efter genomförda intervjuer erbjöds informanterna en transkribering av genomförd intervju för att se att de blivit korrekt återgivna.

Det andra kravet enligt Jacobsen (2002) är informantens rätt till privatliv. För den undersökande betyder detta att den empiriska data inte ska vara skadlig för informanten i avseendet att den är för personlig eller kan avslöja något som är konfidentiellt inom verksamheten (Jacobsen, 2002). Huruvida intervjumaterialet klassas som känsligt är inget undersökarna kan avgöra, vilket höjer kravet på att undersökningen erbjuder informanten samt verksamheten informanten representerar full anonymisering (Jacobsen, 2002).

4 Resultat

I detta kapitel kommer resultatet som erhölls via vår kvalitativa ansats att presenteras. Resultatet presenteras via teman utifrån intervjuguiden, som i sin tur bygger på undersökningsmodellen. Vidare har vi valt att presentera resultatet i tabellform för att på ett enkelt sätt kunna få överblick av informanternas svar och kunna jämföra svaren med varandra. Samtliga intervjuer finns i sin helhet transkriberade som bilagor vilka vi i tabellen refererar till genom att ange vilken intervju och i vilket eller vilka stycken svaret finns. Saknas ett svar från informanten är rutan gråmarkerad.

4.1 Inledning

Tabellen nedan är av inledande natur för att ge inblick i hur verksamheterna arbetat mot tillmötesgående av GDPR generellt, när deras arbete började och om hur väl förberedda de är inför att lagen träder i kraft.

Tabell 4.1: Inledning

Intervjufråga	IF1	IF2	IF3	IF4	IF5
När började ni arbetet mot GDPR?	Påbörjat efter sommaren 2017. (1.10)	Påbörjat vintern 2016. (2.9)	Ingen direkt startpunkt då de jobbat länge liknande uppgifter enligt PuL (3.13)	Började arbetet tidigt 2018. (4.10)	Informanten gick in som projektledare Mars 2017, arbetet började strax innan det. (5.12)
Hur såg förändringsarbetet ut i korta drag?	Gemensamt grupprojekt som drivits centralt. Leverans i fem steg. Arbete med att strukturera processer och styrdokument. Kontroll på flöden i system. (1.10, 1.14)	Uppdelat i två delprojekt. Första: omställningsarbete som organisation. Resultat var anställning av informationssäkerhetssamordnare. Jobba med informationsklassning & policys. Andra delen: Utbildning och migreringsarbete. (2.11)	Hade mycket grundarbete klart kring kataloguseringen av behandling och personuppgifter redan gjort. Fokus har legat på de nya utmaningarna i GDPR. Mycket möda har lagts på att sätta sig in i lagstiftarens andemening. (3.13)	Utfört inventering, tillgångsutvärdering, riskbedömning. Även kartläggning av dataflöden även om det uppdagas nya sådana kontinuerligt. Gäller också delning av uppgifter till leverantörer. Upprättat en personuppgiftsprincip kring alla uppgifter i system. (4.12)	Till en början delades arbetet upp i tre separata projekt, IT, HR och Kundservice. Sedan insåg de att det är verksamhetsfråga och de olika delprojekten slogs samman till ett projekt på avdelningen Affärsutveckling. (5.8, 5.12)
Känner ni er redo?	Majoriteten är på plats med automatiserade rutiner. Några manuella bitar inledningsvis (1.11).	"Vi är inte färdiga, vi är redo" Universitetsvärlden har gemensam samsyn kring problem via maillista. Gemensam inventering, klassificering, beredning, utbildning och personuppgiftsbehandling. (2.13)	Anser att de är så redo som de kan bli. Menar att arbetet kring det här aldrig upphör utan är en cyklisk process. (3.15)	Inte redo och arbetet fortsätter utöver sommaren och hösten med nya verktyg (4.30)	Hävdar att inget företag i hela Sverige är redo. Informanten likställer arbetet mot GDPR med arbete med hållbarhet där det aldrig blir helt färdigt då det hela tiden måste utvecklas. (5.14)

4.2 Personuppgifter och dataportabilitet

Nedan presenteras informanternas svar kring vilka personuppgifter verksamheterna samlar in och hanterar samt vilka som är berättigad flytt vid en dataportabilitetsbegäran. Vidare presenteras svar om verksamheterna erbjuder dataportabilitet samt om de räknar med många dataportabilitetsbegäran.

Tabell 4.2: Personuppgifter och dataportabilitet

Intervjufråga	IF1	IF2	IF3	IF4	IF5
Vad för slags personuppgifter samlar ni in?	Personuppgifter knutna till engagemanget. Kundidentifierare som namn, adress, personnummer och ev. hälsouppgifter. (1.18)	Uppgifter i ladok, uppgifter av de som jobbar på LDC, uppgifter i löneregister, bokningsregister och debiteringssystem. (2.19, 2.21, 2.22).	Beror lite på vad för del av verksamheten samt vad man klassar som personuppgifter. Vanliga personuppgifter som namn, personnummer, adress osv. Även förbrukningsmätvärdet nämns. (3.21, 3.33, 3.37)	Vanligaste person- och namnuppgifter samt rättsuppgifter. Myndighetsutövning i form av ex. färdtjänst därav också hälsodata. Även resehistorik enligt avtal (PUL). (4.16).	Samlar in uppgifter för att identifiera kunden: personnummer, namn, adress, telefon och mail. Även kreditupplysningar, mätdata, ärendeloggar och uppgifter via kundundersökningar. (5.15)
Har ni gjort någon härledning av uppgifterna?	Segmentering inom kundområden för prissättning och mervärde. (1.20)	Utför ingen typ av härledning eller profilering. Ingen raffinering om inte specifika förfrågningar kommer från kunder. (2.20)	Ja. Härledning av uppgifterna görs för marknadsföring och riktad reklamerbjudanden. (3.29)	Analys av köpmönster och hur ofta en kund besöker diverse websida. Finns tankar på att utveckla lojalitetsprogram via analys. (4.20).	Ja. Härledning för marknadsföring och riktade reklamerbjudanden. (5.18
Erbjuder ni dataportabilitet till era användare?	Ja. Detta sker lokalt men med hjälp av verktyg från den centrala organisationen. (1.24).	Möjligheten finns att portera - men inget syfte. Menar att det mer är riktat åt social medier. (2.19)	Ja. Det har de enligt informanten i vissa aspekter redan gjort under många år p.g.a. rådande lagstiftning. Däremot finns svårigheter att identifiera vad kunden vill ha i en begäran i förhållande till GDPR. (3.25, 3.37)	Ja i den mån som är möjligt. Påpekar svårigheterna i form av juridisk komplexitet. (4.24).	Ja då det rådande regelverket inom elbranschen kräver det redan i vissa aspekter. Påpekar dock svårigheten att definierar vad en personuppgift är. (5.22).
Vad för slags uppgifter är aktuella vid dataportabilitet?	Uppgifter som relevanta till kundens engagemang. (1.24)	Personuppgifter ur ladokdatabasen. (2.19)	Förutom klassiska personuppgifter såsom namn, personnummer, adress m.m. Efter diskussion har även information från "Mina Sidor" såsom parametrar i olika val. Även mätetalet är aktuellt. (3.33, 3.37)	Beroende av vilka tjänster som blivit utnyttjade. Uppgifter knutna till registrerat konto är berättigade. Vidare uppgifter i andra system är inte klarlagda om de är berättigade eller inte. (4.28)	I dagsläget är det uppgifter som krävs för att du ska kunna vara kund hos något annat företag (5.24).
Räknar ni med många dataportabilitetsbegäran?	"Jag tror inte det blir en boom direkt. Möjligtvis de kunder som redan har ett horn i sidan mot oss." (1.28)	Kan inte se att det finns mycket i registren som folk vill ha. Räknar inte med många begäran. (2.19)	Nej räknar inte många till början. I jämförelse med registerutdrag så räknar de med färre. Möjligtvis mer i framtiden när kunder förstått värdet av det. (3.31)		Svårt att avgöra, men är säker på att det kommer förekomma 10-tal begäran från "rättshaverister". (5.30).

4.3 Tekniska utmaningar

I tabellen nedan presenteras informanternas svar kring tekniska svårigheter de har upplevt i samband med att erbjuda dataportabilitet, dess format och eventuellt användning av ett API. Vidare presenteras svar kring om det har funnits något tekniskt samarbete eller dialog. Avslutningsvis presenteras informanternas svar kring hur förhållningssättet sett ut kring användandet av Privacy by Design och om det tagits i beaktning vid process- och systemutveckling i avseende att erbjuda dataportabilitet.

Tabell 4.3: Tekniska utmaningar

Intervjufråga	IF1	IF2	IF3	IF4	IF5
Rent tekniskt, vilka utmaningar har ni ställts inför i samband med dataportabilitet?	Tidsaspekten att få ut informationen. Även hur detta ska byggas då många system inte är förberedda arkitektoniskt. (1.30)	Tidsaspekten att få ut uppgifterna. Utmaningar med att veta hur långt ner i systemens hierarkier man hämtar informationen. (2.29, 2.35)	Den största utmaningen är att samla in informationen. Samtidigt som man måste ringa vad kunden kräver dataportabilitet kring och förstå vilken information som kan anses tillhandahållen. (3.33)	Tidsaspekten att hinna få ut personuppgifterna. (4.24). Systemstöd för att kunna hitta alla personuppgifter och komplexiteten av personuppgifterna i systemen. (4.26)	Inte veta hur andras system ser ut och synkronisera med andra företag. Även att pussla ihop vilka olika slags system som finns och vad de innehåller för personuppgifter. (5.31, 5.32).
Vilka utmaningar har ni uppdagat kring vilka format som ska användas och hur har ni ställt er till dessa?	Har ej varit nära den delen av leveransen kring format. Men anser att alla strukturerade format är inläsningsbara på ett sätt eller annat. (1.32)	Kan skicka i vilket nästan vilket format som helst. Ser inga utmaningar med formaten. (2.29, 2.33).	Att först internt enas kring en standard då de har många olika system. Men en vädjan till överordnade Energimyndigheten att som vanligtvis sätter standarden sätta en standard kring det här med. Har även undersökt om XML-format kan vara lämpligt. (3.37, 3.21)	Saknar kompetens kring att hantera format mellan nya och gamla system. Utmaningar med mottagande parts system. Problematik kring mottagarens förmåga att utläsa något ur formatet. (4.30).	Svårt att förstå användningsområde för överförd data i specifikt format. Påpekar även att Officepaketet är ett format som de flesta klarar av att läsa. Menar även att formatet kommer för det mest vara ett enkelt excelblad. (5.36, 5.38).
GDPR rekommenderar API för att förenkla dataportabilitet. Är det något ni gjort eller tänkt göra?	De är inte där i dagsläget men förmodar att det kommer då det finns i det centrala projektets riktlinjer.(1.34, 1.36)	Har inget problem med att använda API. (2.31)	Har haft det i åtanke men efter att ha vägt kostnaden att bygga och vad de tror utnyttjandegraden kommer vara så har de inga planer just nu. Men tror även att funktionaliteten just inte är långt ifrån att kunna leverera detta. (3.41)	Har övervägt det men problematiken ligger i autentisering. (4.34)	Det finns redan till viss del på “Mina Sidor”. (5.40)
Har ni använt tekniska branschstandarder eller följer ni något ramverk kring dataportabilitet?	Informanten vet inte. (1.38)	Använder gemensam mall på samtliga universitet och högskolor i Sverige. (2.13).	Har sedan länge haft standardformat inom branschen p.g.a. rådande regelverk kring det fria elleverantörsbytet. Däremot finns inget uttalat standardformat kring Dataportabilitet utan de väntar och hoppas på att branschorganisationen ska sätta dem. (3.21, 3.37, 3.43)	Försöker hålla sig till sina egna system och rutiner för att först lokalisera alla personuppgifter i omlopp och minimera pappershandläggning (4.36).	Informanten vet inte. (5.44)

Har ni haft något tekniskt samarbete med andra verksamheter inom samma sektor kring dataportabilitet?	Informanten vet inte. (1.38)	Samarbetar med andra Universitet och högskolor i Sverige. (2.13)	Etablerat samarbete sedan tidigare p.g.a. rådande regelverk. Däremot inget tekniskt samarbete kring GDPR eller Dataportabilitet. (3.21, 3.37, 3.43)	Inget samarbete har upprättats utöver samarbete kring databaser som används. (4.36). Brytningspunkt då många använder egna tekniska lösningar. (4.36)	Existerar sedan tidigare ett samarbete mellan energibolag där kunden enkelt kan byta leverantör. Inget tekniskt samarbete riktat mot just GDPR och dataportabilitet har upprättas. (5.42, 5.44)
Hur förhåller ni er till Privacy by Design? Tar ni det i beaktning vid utveckling av nya system eller processer? **Är det något som har tagits i åtanke vid att erbjuda dataportabilitet?**	De har inom bank-delen använt sig av PbD länge. Stor del när kravställning för nya system sker. Däremot har de ej applicerat nya systemlösningar inför GDPR utan en genomgång av redan applicerade lösningar verkligen fungerar har gjorts. (1.56)	Har hållit i GDPR-utbildning där PbD förespråkats i form av uppgiftsminimering, anonymisering och pseudonymisering. Har gått igenom system för att se till att man inte hanterar mer uppgifter än vad man behöver. (2.59, 2.61)	Då verksamheten är styrkt av att de är en samhällsviktig funktion så har de haft rigorösa krav och denna tankegång sedan länge. De har även stärkt PbD-tankegången ytterligare inom verksamheten inför GDPR. En genomgång av etablerade system har gjorts och vissa svagheter i ett integritetsperspektiv har hittats och åtgärdats. (3.56)	Arbetar med Privacy by design som förhållningssätt i olika utvecklingsprogram. För att underlätta för Skånetrafiken och kunden. Dock inte kommit önskvärt långt (4.52)	Jobbar mycket med Privacy By Design i säkerhetssyfte. Har personal och externa jurister som ställer stora krav på företagets egna system och processer men också på systemleverantörerna. Ställer höga krav på integritet och säkerhet i systemen som hanterar deras kunder och anställda. (5.58)

4.4 Organisatoriska utmaningar

I tabellen nedan presenteras utmaningar som informanterna menar att sin verksamhet ställts inför för att kunna erbjuda dataportabilitet, samt vilka förändringar som behövs göras för att möta kravet. Vidare presenteras svar om något systemstöd ämnats att tas i bruk för automatisering av bearbetning av dataportabilitetsbegäran. Tabellen visar även informanternas svar om det förekommit samarbete på organisatorisk nivå inom respektive sektor för att hantera dataportabilitetsbegäran.

Tabell 4.4: Organisatoriska utmaningar

Intervjufråga	IF1	IF2	IF3	IF4	IF5
Rent organisatoriskt vilka utmaningar har ni ställts inför i samband med dataportabilitet?	En utmaning har varit att få medarbetare att förstå varför de gör detta och vad som landar på varje individ. Ansvaret över hela förloppet i kunddialogen. (1.58)	Tidsspillan via oupprättade policys kring hur en begäran ska behandlas. (2.47)	Att förstå vad kunden lägger i ordet dataportabilitet. Vad kunden egentligen frågar efter. (3.62).	Veta vilket IT-stöd som behövs. Den omvända bevisningen är också en stor utmaning. (4.38).	Hitta vem som är ansvarig eller att utse den som är ansvarig då många vill trycka ansvaret ifrån sig. (5.48)
Har ni behövt göra några organisatoriska förändringar i samband med att kunna erbjuda dataportabilitet?	Genomföra sammanställningar och identifieringar i hur processer ser ut i hantering och kunddialog. Även ta reda på vilken information och personuppgifter som hanteras och i vilka register de finns. (1.40)	Ingen specifika förändringar på högre nivå har gjorts för just aspekten kring dataportabilitet. (2.47)	Dataportabilitetsfrågan har nedprioriteras något i verksamheten. En taskforce för frågan har däremot satts ihop Troligtvis kommer det bli en manuell rutin att besvara en förfrågan. Även utbildning av medarbetare har initierats. (3.44, 3.46)	Gjort nya riktlinjer och policys kring de manuella processerna för en begäran. (4.42).	Har tagit fram flera lager av riktlinjer och rutiner kring GDPR och då i förlängningen dataportabilitet. Även utsett två personer på kundservice som ska hantera förfrågningar till en början. (5.30, 5.46)
Har det behövs nya processer för att kunna svara på en dataportabilitetsbegäran?	Nya processer för att säkerhetsställa att rätt information skickas i rätt kanal. (1.46, 1.48)	Inga nya processer i ändamålet att svara på just dataportabilitetsbegäran. Vid en eventuell begäran kommer det skötas manuellt (2.49).	Ingen ny process har skapats utan det blir en manuell rutin till att börja med. Däremot har de påbörjat arbete med att identifiera liknande metoder från olika system för att underlätta en export dataportabilitetsmässigt. (3.44)	Nya manuella processer är på plats. Systemmässiga processer kommer ta lång tid. Autentiseringsprocessen är den viktigaste. (4.42).	Inga nya processer har upprättats specifikt för dataportabilitet men två personer har utsetts till ansvariga för detta. (5.30).
Är några av processerna automatiserade? Ska de bli?	Tekniska lösningar har skapats för underlätta förflyttning, hantering och bearbetning av informationen. (1.46)	Vid många eventuella likartade begäran kommer det behövas automatisering. (2.51).	Manuell process till en början. Ingen kommentar kring automatisering. (3.44)	Det är tänkt att de nuvarande manuella processerna ska systematiseras så fort man kan säkerställa en autentisering. (4.42, 4.45).	Inte för tillfället men de arbetar simultant med vad de kallar "Kraftringens processer" där manuella processer först in och i slutändan ska automatiseras. (5.52)
Har ni haft något organisatoriskt samarbete med andra verksamheter inom samma sektor kring Dataportabilitet?	Nej, inte utifrån informantens vetskap. (1.50)	Inget uttalat samarbete just i syftet att svara på dataportabilitetsbegäran. (2.43)	Inget samarbete än så länge kring GDPR och Dataportabilitet. Samarbete som i vanliga fall är vanlig i andra ärenden såsom regleringskrav. (3.48)	Inte kring dataportabilitetsbegäran specifikt. Dock kring processer i utveckling av biljettsystem, samt dialog med andra företag vad det är för personuppgifter som ska överföras från ett system till ett annat om en kund vill åka från ex. Skåne till Småland. (4.47).	Verksamheten har etablerade organisatoriska samarbeten sedan tidigare i branschen. Ett GDPR-samarbete etablerades som sedan avslutades. Inget samarbete kring Dataportabilitet finns. Informanten påpekar att detta borde branschorganisationen ta tag i. (5.26, 5.54)

5 Diskussion och Analys

I detta kapitel analyserar vi den insamlade datan och ställer den mot teorin vi presenterat i litteraturgenomgången och presenterar eventuella skillnader, likheter och andra fynd.

5.1 Interoperabilitet och dataportabilitet

Inom artikel 29-gruppens riktlinjer för dataportabilitet förespråkas starkt interoperabilitet för att underlätta och möjliggöra behandling av dataportabilitetsbegäran. Där uppmuntras verksamheter att etablera branschsamarbete och sätta standardformat. Av de fem informanterna var det bara IF2 som hade ett uttalat samarbete med andra verksamheter i sin bransch. Informanterna IF3 och IF5, som båda är del av samma bransch, har sedan länge haft etablerat samarbete och har uppnått interoperabilitet inom delar av verksamheten. Däremot har ingen ansats mot interoperabilitet gentemot dataportabilitet upprättas. Resultatet visar härigenom på, som flertalet informanter nämnt, att en stor del av arbetet mot att erbjuda dataportabilitet inte har varit att upprätta samarbete och standarder med andra parter, utan fokus har varit på andra aspekter.

Xia et al (2014) påpekar att interoperabilitet är en komplex förmåga, då en av många förutsättningar är att först kunna hantera sina interna dataflöden. Detta bekräftas av IF3 där informanten menar att deras egen verksamhet först måste enas kring en gemensam standard av format, då de har en stor mängd system med olika format. Även IF4 påpekar problematiken kring kartläggning av dataflöden då det kontinuerligt uppdagas nya flöden. Vid frågan kring användandet av tekniska branschstandarder menade även IF4 att de först ska försöka hantera sina egna system och rutiner för att lokalisera personuppgifter. Detta anser vi till viss del förklara bristen på ansats till samarbete då många verksamheter fortfarande arbetar internt med hantering av sina egna dataflöden.

Problematiken kring interoperabilitet beskrivs också av Chen & Daclin (2006) som olika barriärer. De beskriver olika typer av barriärer, såsom exempelvis tekniska, vilka kan gestaltas genom avsaknad av kompatibla standarder mellan verksamheter. IF5 menar också att just bristen på att ha likartade rutiner och system mellan olika parter kan försvåra synkroniseringen av personuppgiftsdelning vid en dataportabilitetsbegäran. Dock påpekar IF1 att ett av de största problemen ligger på en djupare nivå inom verksamheterna. IF1 menar att system inte är redo på arkitektonisk nivå för att effektivt kunna få ut uppgifter och föra dessa vidare till en annan aktör. Detta påvisas även av IF2 som talar om hur svårt det är att veta hur långt ner i systemens hierarkier man ska hämta uppgifter. Problematiken ser vi kan härledas till vad Allen et al (2014) menar kring utvecklingen av system, där fokus inte varit på att systemen ska vara flexibla och anpassade för gränsöverskridande informationsdelning.

Däremot påpekar Allen et al (2014) och Cimander et al (2011) att det är av vikt att inte bara se interoperabilitet som ett problem vars lösning enbart är teknisk. Något som även stöds av Chen & Daclin (2006) med vad de kallar de syntaktiska och semantiska barriärerna. Barriärerna uppstår när det inte finns någon entydig och klart definierad betydelse av informationen som delas. Detta ser vi stöds av IF3, IF4 och IF5 där de påpekar problematiken kring vad just personuppgifter betyder, både ur ett legalt men också ett användarperspektiv.

IF5 uttryckte sig under intervjun frågande:

"Nu tycker jag återigen man är i den här situationen, hur definierar vi vad en personuppgift är?" (5.22)

IF2 påpekar dock att de har tillsammans med andra verksamheter i samma bransch skapat en mall vilken de använder för att etablera en samsyn. På så sätt ser vi att de kan få klarhet i definitioner och betydelser och till viss del överkomma den semantiska och syntaktiska barriären som Chen & Daclin (2006) nämner.

Vidare påpekar Chen & Daclin (2006) och Cimander et. al (2011) att problematik kan finnas på en organisatorisk nivå som kan försvåra interoperabilitet. Något som IF5 nämnde var när ansvaret av GDPR och således dataportabiliteten skulle fördelas. IF5 nämner att projektet först var tredelat inom organisationen där HR, kundservice och IT hade egna projekt. Vidare menar IF5 att många ville trycka ansvaret ifrån sig och inte ta tag i frågorna. För att underlätta projektstyrningen slogs de tre olika projekten samman till ett större projekt.

Sammantaget kräver litteraturen att många olika komponenter måste vara på plats och att många barriärer måste tas igenom för att uppnå interoperabilitet kring dataportabilitet. Den insamlade empirin tycks te sig på det viset att fokus initialt ligger internt för de tillfrågade verksamheterna. Interoperabilitet kan således vara något som kan växa fram allt eftersom verksamheterna nått längre i deras interna arbete med dataportabilitet och GDPR inom den egna organisationen. Baksidan av detta kan däremot leda till att verksamheterna utvecklar välförankrade standarder och rutiner internt, vilket i slutändan kan försvåra interoperabiliteten.

5.2 Tekniska utmaningar och Privacy by Design

För att en dataportabilitetsbegäran ska kunna besvaras krävs det att flertalet tekniska funktioner och processer finns på plats. Samtliga informanter menar att en stor teknisk utmaning är att lokalisera var uppgifterna finns, och sen avgöra vad det är för typ av uppgifter som finns i systemen inom den satta tidsfristen. I tillägg påpekar IF1 att system inte är arkitektoniskt byggda för att lösa en begäran effektivt, och IF2 menar det är svårt att avgöra hur långt ner i systemens hierarkier begäran ska nå.

Då lagen inte trätt i kraft ännu är det svårt att veta till vilken frekvens dataportabilitetsbegäran kommer ske. Ovissheten har gjort att IF2 och IF3 i utgångspunkten kommer sköta sina inkommande begäran manuellt och från fall till fall. De ser inte relevansen med att automatisera hanteringen, eller utveckla något nytt systemstöd innan det finns en tydlig omfattning av hur många begäran som kommer komma in.

Vidare råder ingen konkret konsensus kring vilka format som ska användas vid en dataportabilitetsbegäran. Rekommendationen ur GDPR påpekar, som nämnt tidigare, att formatet ska vara i ett strukturerat, allmänt använt och maskinläsbart format. Resultatet i vår studie presenterar vitt skilda svar kring hur detta tolkats av informanterna. IF2 menar att det inte finns några hinder i att utföra en begäran i nästintill vilket strukturerat format som helst, medan IF3 undersöker möjligheten till att använda XML. Dock påpekar IF4 och IF5 att problematiken

mer ligger i mottagarens förmåga att utläsa något ur ett visst format. IF4 beskrev problematiken följande under intervjun:

"Ska det vara CSV-fil eller det ska kunna läsas i klartext, eller du ska själv tyda det? Om du tittar på en person, oaktat vem det är så ska denne kunna se och förstå vad som står på dessa sidor" (4.30)

Lagen förespråkar också användningen av API som verktyg för att underlätta processen med begäran, vilka IF2 och IF5 menar de har förutsättningar att konstruera. IF3 och IF4 menar att det har övervägts men problematiken ligger i förväntad användningsfrekvens kontra kostnad samt hur man ska hantera autentiseringen som är en central skyldighet för personuppgiftsansvariga. Något som vi möjligtvis anser kan ändras efter lagen trätt i kraft, då man i större utsträckning kan uppskatta antalet begäran.

GDPR förespråkar inbyggd integritet, vilket också kallas Privacy By Design, vilket enligt Cavoukian (2012) kan ses som ett ramverk eller strategi för hur integritet inbäddas i verksamheters systemutveckling och processer. Då samtliga informanter menar att nya tekniska lösningar inte upprättas för att svara på just dataportabilitetsbegäran så har däremot tankesättet Privacy By Design varit väletablerat under lång tid. Dock menar IF4 att utvecklingsprogram med Privacy By Design i fokus inte kommit önskvärt långt. Däremot har IF2s verksamhet arbetat med Privacy By Design i utbildningssyfte där mycket av vad Diaz et al (2011) påpekar kring data minimering tas i beaktning. Då Schaar (2010) påpekar att system ska byggas för nutida problem så menar han även att systemen ska kunna handskas med framtida problem. Därav anser vi om verksamheterna arbetat i större utsträckning med tankesättet vid både process och systemutveckling, i form av uppgiftsminimering, radering, anonymisering och klassificering kunde en dataportabilitetsbegäran behandlas mer effektivt. Något som vi anser verksamheterna bör ha i åtanke vid utveckling och vidareutveckling av system. Cavoukian (2012) menar då i utvecklingssyfte att verksamheter kan använda sig av sju stycken principer för att minimera säkerhetsriskerna i sina system och öka fokus på den personliga integriteten. Dock kan det ses som en väldigt komplicerad uppgift att ta sig an då flertalet informanter påpekar att själva antalet system är svårhanterligt.

5.3 Organisatoriska utmaningar och förändringar

Samtliga tillfrågade verksamheter har fått genomgå stora organisatoriska- och processorienterade förändringar inför tillmötesgående av GDPR. Däremot när det kommer till just dataportabilitet verkar det som verksamheterna har nedprioriterat frågan, vilket IF3 nämner rakt ut vid intervjun. Endast IF1 och IF4 utav de tillfrågade nämner att en specifik process har skapats för att hantera dataportabilietsbegäran. Samtliga informanter menar dock att de kommer erbjuda dataportabilitet, även fast syftet kan verka oklart enligt IF2. Anledningen till detta kan vara att ingen av informanterna anser att de kommer få hantera speciellt många dataportabilitetsbegäran. IF5 menar att det är svårt att avgöra hur många som kommer begära dataportabilitet, utan tänker att de kommer få ett 10-tal begäran av "rättshaverister". Vidare uttryckte IF1 en liknande åsikt och sa under intervjun:

"Jag tror inte det blir en boom direkt. Möjligtvis de kunder som redan har ett horn i sidan mot oss" (1.28)

När informanterna blev tillfrågade kring vad de anser vara de organisatoriska utmaningarna de ställs inför svarade de alla olika. IF1 menar att svårigheten ligger i att motivera och få medarbetare att förstå varför de utför och erbjuder dataportabilitet. IF5 nämner svårigheter i att hitta vem som ska ha ansvar för frågan. Något som kan ses i linje med Harmons (2014) problematik för processer på en låg nivå i processhierarkierna. För att åtgärda detta menar Harmon (2014) att arbetsbeskrivningar och träningsprogram kan utvecklas samt rollfördelningen analyseras för att förstå vem som lämpligast ska bära ansvaret.

Vidare kan komplexitetsgraden för dataportabilitetsprocessen diskuteras. Harmon (2014) menar att processer ligger på ett spektrum av enkla processer, komplexa processer och väldigt komplexa processer. Harmon (2014) menar att enkla och till viss del mer komplexa processer kan automatiseras. Däremot är det bara IF1 och IF4 som har skapat någon slags process kring hur de ska hantera en dataportabilitetsbegäran och således flyttat processen mot en enklare process med möjlighet till automatisering. IF2, IF3 och IF5 har som nämnt tänkt att hantera begäran mer manuellt och från fall till fall. Vilket enligt Harmon (2014) kan ses som en väldigt komplex process där mycket tid kommer gå åt på att avgöra hur hanteringen av dessa ska gå till. Dessa är enligt Harmon (2014) samtidigt väldigt svåra att automatisera.

Däremot menar samtliga informanter att de utvärderat olika tekniska lösningar och utmaningar i att få ut den registrerades personuppgifter ur systemen. Därav anser vi att det är rimligt att anta att ingen av verksamheterna kommer börja denna process från grunden utan att en viss tanke kring hur detta ska ske är etablerad.

Moran & Brightman (2000) betonar att förändringsarbete inom verksamheter är icke-linjärt med ingen tydlig definierad start eller slutpunkt då den sker cykliskt. Något som både IF3 och IF5 nämner. IF5 nämner att deras förändringsarbete mot GDPR och dataportabilitet kan likställas med deras arbete för hållbarhet där man aldrig riktigt kan bli färdig. Detta menar Moran & Brightman (2000) mynnar ut i deras ramverk ”the change management cycle” med fyra faser. Utifrån informanternas svar kan man utläsa att de olika verksamheterna har kommit olika långt i förhållande till de olika faserna. IF2, IF3 och IF5 bedömer vi fortfarande vara i den första fasen av cykeln, vilket Moran & Brightman (2000) menar är att förstå den nuvarande situationen. Som de påpekar finns svårigheter för förändringsledarna, antingen informanten själv eller dess projektgrupp, att greppa vad för slags uppgifter den registrerade vill ha vid en dataportabilitetsbegäran samt hur och i vilket format. IF3 och IF5 nämner en önskan att deras gemensamma branschorganisation ska sätta riktlinjer för att de enklare ska kunna förstå den nuvarande situationen. Även svårigheter att veta hur de ska identifiera samt exportera den registrerades uppgifter nämns.

De har således svårt att nå nästa fas i cykeln, vilket Moran & Brightman (2000) menar är att bestämma det önskade tillståndet samt att utveckla en förändringsplan för att nå dit. Något som både IF1 och IF4 nämner att de har lyckats med. Både IF1 och IF4 har således utvecklat en förändringsplan för att implementera nya processer i syfte att besvara en dataportabilitetsbegäran. De har följaktligen börjat etablera denna förändring i verksamheten vilket Moran & Brightman (2000) menar är den tredje fasen i cykeln. Moran & Brightman (2000) presenterar även problematik kring den tredje fasen vilket är att nå kritisk massa, det vill säga att få medarbetare att upprätthålla förändringen och att acceptera den. Detta är något som IF1 också nämner som problematiskt, där utmaningar är att få medarbetare att förstå varför de erbjuder dataportabilitet samt vilket ansvar det innebär.

Den slutgiltiga fasen i cykeln innan allt itereras är enligt Moran & Brightman (2000) att följa upp och stabilisera resultat. Detta är en fas i cykeln ingen verksamhet för tillfället uppnått då det inte finns något resultat att hämta då lagen ännu ej trätt i kraft.

6 Slutsats

I detta kapitel sammanfattar vi vad studien resulterat i utifrån empirin och tidigare litteratur i ämnet. Studien ämnade att svara på följande forskningsfråga:

Vilka tekniska och organisatoriska utmaningar ställs verksamheter inför för att kunna erbjuda dataportabilitet i samband med införandet av GDPR?

Vid införandet av GDPR och den nya rätten till dataportabilitet kommer det krävas av verksamheter att se över sin hantering av personuppgifter. Vidare kommer verksamheter tvingas kunna identifiera och exportera personuppgifter som den registrerade har rätt till vid en dataportabilitetsbegäran. Då verksamheter inte tidigare varit ålagda att erbjuda dataportabilitet ger det nya dataportabilitetskravet upphov till en ny problematik med flertalet olika aspekter. Vår undersökning visar på flera utmaningar av såväl teknisk som organisatorisk natur för att kunna svara på en dataportabilitetsbegäran.

Vi ser i vår undersökning att de större tekniska utmaningarna verksamheterna ställts inför är att få ut de uppgifter som ska vara med vid en dataportabilitetsbegäran inom den tidsram som lagen kräver. Användandet av flertalet system samt att systemen generellt inte är förberedda arkitektoniskt för extrahering av personuppgifter ser verksamheterna som de största utmaningarna. Formatet för dessa personuppgifter ser verksamheterna inte som en större utmaning, utan problematiken anses ligga mer i den mottagande partens förmåga att utläsa dessa. Vidare anses inte rekommendationen kring att utveckla ett API för att förenkla exporten av personuppgifter som någon större utmaning för verksamheterna. Däremot sågs den förväntade nyttjandegraden låg gentemot utvecklingskostnaden.

Undersökningen konstaterar att verksamheterna står inför flertalet organisatoriska utmaningar, där en av dessa innefattar hur verksamheter ska förstå vad en dataportabilitetsbegäran egentligen syftar till och innefattar. Något som vi också ser ger sig i uttryck av att verksamheter poängterar svårigheter med att motivera och tydliggöra för sina anställda varför dataportabilitet ska kunna erbjudas. Vårt resultat visar också tydligt att några av verksamheterna ställts inför problemet med att tydliggöra vem som bär ansvaret för att hantera dataportabilitetsbegäran inom organisationen. Sammantaget visar vår undersökning att inte ens hälften av verksamheterna upprättat processer i syfte att hantera en dataportabilitetsbegäran. De tekniska och organisatoriska utmaningarna ligger även i linje med de barriärer som teorin presenterar kring att uppnå interoperabilitet.

Ur den kvalitativa ansatsen kan vi även utläsa att verksamheter inte prioriterat dataportabilitetskravet i GDPR. Generellt har verksamheterna inte vidtagit några större tekniska eller organisatoriska förändringar för att möta lagkravet. Ansatsen verksamheterna gjort är mer riktad åt andra krav i den nya förordningen, då just dataportabilitet inte ses som väldigt applicerbar på just deras verksamhet. Verksamheterna uttrycker tydligt att det inte finns någon hög förväntad grad av dataportabilitetsbegäran och några menar även att dom inte ser något syfte med en sådan. Något som kan anses oroväckande ur ett medborgarrättsligt perspektiv.

7 Förslag på vidare forskning

Då vår forskning undersökt vilka möjliga utmaningar verksamheter ställs inför i avseendet att kunna erbjuda dataportabilitet, så visar resultatet mer mot att frågan till en viss grad är bortprioriterad. Verksamheterna påpekar att deras förväntningar på hur många dataportabilitetsbegäran som kommer inkomma är låg. Vidare forskning hade därför kunnat utföras kring samma aspekter dock efter att lagen trätt i kraft och varit gällande under en längre tidsperiod. Vi tycker också det vore intressant att vidare undersöka och jämföra verksamheter i vår studie med andra verksamheter som förväntar sig stora kvantiteter av dataportabilitetsbegäran. Det hade varit av intresse att se skillnaderna med istället tydliga processer samt anpassad teknisk infrastruktur för ändamålet.

Appendix

Intervjufrågor

Inledande frågor

- Är det okej att vi spelar in?
- Önskar du vara anonym?
- Utbildning och bakgrund?
- Roll i verksamheten?
- Erfarenhet av tidigare förändringsarbete?
- Roll i förändringsarbetet?
- Omställningsarbete kring GDPR generellt
- När började ni arbetet mot GDPR?
- Hur har ert förändringsarbete sett ut i korta drag?
- Känner ni er redo?
- Har ni använt er av konsulter?

Vårt fokus - Dataportabilitet

- Vad för slags personuppgifter samlar ni in?
- Vad för slags hantering sker av dem, gör ni några avledda eller härledda analyser av dessa? T.ex profilering?
- Är du bekant med rätten till dataportabilitet?
- Erbjuder ni dataportabilitet för era kunder/användare?
    - Om nej - varför?
    - Om ja - vad för slags uppgifter är berättigade till förflyttning inom er organisation?
- Räknar ni med många dataportabilitetsbegäran?

Tekniska frågor

- Rent tekniskt, vilka utmaningar enligt dig har ni ställts inför i samband med att kunna erbjuda dataportabilitet?
- GDPR är relativt otydligt kring vilka format som bör användas och definierar det som "*i ett strukturerat, allmänt använt och maskinläsbart format"*. Vilka utmaningar har ni uppdagat kring just vilka format som ska användas och hur har ni ställt er till dessa?
- GDPR rekommenderar API för att förenkla dataportabilitet. Är det något ni gjort eller tänkt göra?
- Har ni använt tekniska branschstandarder eller följer ni något ramverk kring dataportabilitet?
- Har ni haft något tekniskt samarbete med andra verksamheter inom samma sektor kring dataportabilitet?
    - Om nej - varför tror du det?
    - Om ja – utveckla gärna

Organisatoriska och processorienterade frågor

- Rent organisatoriskt eller processorienterat, vilka utmaningar har ni ställts inför i samband med att kunna erbjuda dataportabilitet?
- Har ni behövt göra några organisatoriska förändring i samband med att kunna erbjuda dataportabilitet?
    - Vilka i så fall?
- Har det behövs nya processer för att kunna svara på en dataportabilitetsbegäran?
- Är några av processerna automatiserade? Ska de bli?
- Har ni haft något organisatoriskt samarbete med andra verksamheter inom samma sektor kring Dataportabilitet?
    - Om nej: Har någon dialog i huvudtaget etablerats?
    - Om Ja: Hur och vilka?
- Privacy by design är strategi/tankesätt som förespråkas av GDPR. Är du bekant av Privacy by Design?
- Hur förhåller ni er till privacy by design som strategi eller ramverk? Tar ni det i beaktning vid t.ex. utveckling av nya system eller processer?
- Är det något som har tagits i åtanke vid att erbjuda dataportabilitet?

Avslutning

- Vad enligt just dig personligen har varit den största utmaningen med att kunna erbjuda dataportabilitet?
- Önskar du att få transkriptionen av intervjun?

Intervjutranskriberingar

Intervju 1 – Informant 1 – Företag A

Intervjuare: Jesper Fransson (JF) och Edvin Blomberg (EB)
Verksamhet: Bank och försäkringsbolag
Informant: Informant 1 (IF1)
Roll: IT-Chef
Plats: Verksamhetens kontor i Helsingborg
Tid: Onsdagen den 2 maj 2018, 09.00-09.40.

1.1 JF: Så, då hade vi en liten inledande fråga här: Som sagt är det okej att vi spelar in det här? Önskar du vara anonym?

1.2 IF1: Jadå.

1.3 JF: Vi tänkte börja med lite grundläggande frågor om dig. Vad har du för utbildning och bakgrund, inom din roll?

1.4 IF1: Jag är systemvetare i botten, från Lunds universitet. Och sedan lite påbyggnadsutbildningar som väl anställd sen. Certifierad CRO via dataföreningen har jag gått och många sådana här internutbildningar, men certifierad CRO är en del och affärsledarskap och IT-chef är en del som jag har lagt på i efterhand.

1.5 JF: Vad är din övergripande roll i verksamheten?

1.6 IF1: IT-Chef i dagsläget för *Företag A* och ansvar för IT- drift, förvaltning och support.

1.7 EB: Är det olika IT-avdelningar för olika delar inom *Företag A* så att säga?

1.8 IF1: Ja, *Företag A* är ju en federation. Vilket innebär att varje *länsfilial* är sitt egna bolag med egen styrelse och egen VD. Och så har vi ett gemenskapt ägt Servicebolag i federationen som heter *Företag A AB* som då levererar i princip alla system som har med kund att göra, bank, liv och försäkring.

1.9 JF: Nu handlar ju vår uppsats kring GDPR och dataportabilitet. Så vi tänkte först ställa någon fråga kring ert omställningsarbete kring GDPR generellt. När började er omställningsarbete?

1.10 IF1: Vårt arbete kring detta påbörjade vi efter semester i fjol 2017, så vi började ganska tidigt med det. Insåg att det är väldigt mycket arbete som måste gås igenom. Framförallt strukturer på processer och styrdokument som måste ligga till grund för arbetssätten. Men även en hel del arbete kring våra system och säkerställa att vi har kontroll på alla flödena i systemen.

1.11 JF: Känner ni er redo nu?

1.12 IF1: Ja absolut är vi redo. Men det är alltid stressigt inför liksom, vi vill vara säkra på att allting är på plats. Och ja, jag skulle säga att absolut majoritet är på plats. Med automatiserade rutiner. Sen är det lite bitar som blir manuella bitar inledningsvis men framförallt att vi har kontroll på flödena och processerna.

1.13 JF: Har ni hyrt in mycket experthjälp för det här externt?

1.14 IF1: Vi har ju drivit detta i fedarationen som ett gruppgemensamt projekt vilket innebär att vi har ett huvudprojekt som vi kallar det för som sitter centralt på *Företag A AB*. Det är vårt servicebolag som bistår med, i princip allt, grundmaterialet som vi behöver göra. Hur ska våra olika leveranser se ut, vi har delat upp leverenserna i fem steg har jag för mig. Leveranspaket ett till fem, vad vi ska ha på plats vid vilken tidpunkt för att säkra att vi följer projektplanen. Så därifrån har vi fått mycket och har då arbetat igenom detta på ett enhetligt sätt inom federationen.

1.15 JF: Vad har varit din största roll inom förändringsarbetet mot GDPR-compliance.

1.16 IF1: Det är att säkerställa de system vi har i lokal leverans på *Företag A* och det är framförallt då filprint, printern är inte så noga det här fallet kanske men filytan. Hur hanterar vi dem, hur sörjer vi för att verksamheten vet vad de ska gallra, hur ska de loggföra den information de har som någonstans har behandling av personuppgifter så var har det känt. Sen är det säkerhetsställa de lokala systemen som vi har på ekonomi, analys, telefoni osv. Att vi har systemrutiner på plats och i förstahand uppdateringar av systemen så att vi kan automatisera processen, antingen right to be forgotten eller anonymiseringen och sen utöver det då gallringen, när gallra datan. Och så kommunikationen mot verksamheten då om hur önskar informationsägarna sin information gallrad för det är ju inte IT, för GDPR är inget IT-projekt som jag ser det, det är ett verksamhetsprojekt.

1.17 JF: Nej precis. Nästa del handlar lite mer om vårt fokus som är just dataportabiliteten. Vi tänkte först fråga, vad är det för slags personuppgifter som ni samlar här på *Företag A*?

1.18 IF1: Det vi samlar in är ju det som direkt är knutet till engagemanget. Så på försäkringssidan så måste vi kunna identifiera kunden, objekten som försäkras, adresserna. Så personuppgifterna, namn, personnummer, kontaktyta, telefon, mail, adress. Det är dem primära som samlas in. Vissa delar har vi känsliga uppgifter på, där vi pratar livförsäkringar och vi pratar låneskydd och lite sådanhära bitar så har vi ju hälsouppgifter som också kanske behöver ingå i vissa sammanhang. Och det har ju med vad för slags produkt som kunden köper av oss. Då behöver vi ju veta mer om kunden för att kunna göra en bra leverans.

1.19 JF: Gör ni några härledda analyser av era personuppgifter ni har? T.ex profilering?

1.20 IF1: Ja alltså om vi tänker på hur vi jobbar med segmentering. Så ja, vi tittar ju på segmentering, kanske inte enkom kunden specifikt men områdena där kunden bor. Detta för att hitta den här typen av kvarter eller den här typen av läge i kvarter som riskerar inbrott, vissa delar av vissa områden. Där kan man se här var sker våra inbrott någonstans, hur behöver prissätta för att få teckning för de kostnaderna som kommer på engagemanget. Men de görs ju utifrån områdena, de är ju inte individen i sig, vi vet ju hur många försäkringstagare vi har i ett område men det är ju området som är intressant det är inte personen som sådan utan det är områdena. Just för att hitta rätt segment eller vi vill sälja nya produkter så då också utifrån vad har vi för segment och kunder i det här området. Vad är intressant för att verkligen ge

kunden ett mervärde för det de köper av *Företag A* så vi har trygga kunder? Det är tryggheten vi säljer.

1.21 JF: Är du bekant med rätten till dataportabilitet i GDPR?

1.22 IF1: Ja, det ska jag vara hyfsat.

1.23 JF: Hur kan ni erbjuda era kunder/användare dataportabilitet om vill flytta eller få ut sina uppgifter?

1.24 IF1: Om du vill ha ut sina uppgifter så är det en del i sig. Portabiliteten hanterar vi ju faktiskt i och med att det som rör kunden utifrån engagemangen; bank, försäkring och liv, är ju våra centrala system. Så där också har vi ju byggt portabilitetsbitarna utifrån den centrala leveransen. Så det är ju inte vi lokalt som hanterar hur vi får ut den, vi har ju verktygen men det är på centrala organisationen uppe på *Företag A AB* som bygger lösningen på hur vi får ut information och kan flytta den.

1.25 JF: Vad är det för slags uppgifter som är berättigade till förflyttning för en användare?

1.26 IF1: Ja kunden har ju rätt att veta vad är det för information vi lagrar om dem. Där kan vi ju inte ha dolda agendor så att säga. Vi har ju en full transparens genom våra kundsystem och uppgifter som vi kan spara där är det ju sådana som har med engagemangen att göra. Det vi har gjort tydligare nu det är att all form av fritext eller anteckningsfält som finns inbyggda i de flesta system, dem har vi kommunicerat att de ska inte användas. Just för att säkerställa att här inte kommer information som inte är relevant för engagemanget. Därför är det bättre är det bättre att stryka hela den användningen av fritextfält.

1.27 JF: Jaha smart! Nu efter 25 maj, räknar med ni med många dataportabilitetsförfrågningar?

1.28 IF1: Jag tror inte det blir en boom direkt. Möjligtvis de kunder som redan har ett horn i sidan mot oss. De har ju det förmodligen för att de inte varit nöjda med en leverans i ett försäkringsärende och de är redan på oss om lite olika saker, alltså deras synpunkter. Då fortsätter vi hantera dem på samma sätt. Så här gör vi ingen skillnad egentligen på hur vi jobbar med kunden idag som vi gjorde tidigare, kunden har rätt att få svar på sina frågor på ett tydligt och konstruktivt sätt. Så där är ingen skillnad egentligen.

1.29 JF: Vi tänkte gå vidare till lite mer tekniska utmaningar. Vilken, rent tekniskt, är den största utmaningen ni haft för att erbjuda kunna erbjuda dataportabilitet?

1.30 IF1: Det är tidsaspekten i att få ut informationen. Hur bygger vi detta? För det ju inte många system som är förberedda arkitektoniskt för att hantera det på det sättet. Så det är ju definitivt en utmaning. Vi har ju faktiskt hyfsat bra tid på oss att samla uppgifterna och sammanställa dem och lämna av till kund eller den nya motparten. Sen jag undrar jag hur mycket kunden egentligen vet därute; att vad kan jag begära och varför ska jag begära det? Det är ju en sak att om man inte är kund här längre, då ska man kunna lita på att mina uppgifter plockas bort efter X antal dagar, månader eller år beroende på vilket engagemang man har haft. Samtidigt som vi har rätt att hålla vissa uppgifter utifrån vad det är för typ av engagemang kunden har haft, så här finns faktiskt en laglig aspekt på att vi får hålla de här uppgifter och vi måste hålla dem i vissa aspekter.

1.31 JF: I just dataportabilitetsparagrafen så finns en det en rekommendation när det kommer till format, att det ska vara i ett strukturerat, allmänt använt och maskininlästbart format. Har ni haft några utmaningar i att veta vilket format ni ska använda när ska besvara en dataportabilitetsförfrågan?

1.32 IF1: Det jag tror jag inte, jag är inte så nära den delen av leveransen då den sker från vårt servicebolag. Så nej, jag är inte helt klar på hur den är strukturerad, men de flesta strukturerade format är ju inläsningsbara på ett eller annat sätt.

1.33 JF: En annan rekommendation som står i lagen är att eventuellt bygga ett web-API där kunder kan hämta?

1.34 IF1: Där är vi inte i dagsläget.

1.35 EB: Men är det något ni har tänkt att bygga?

1.36 IF1: Det förmodar jag helt klart utifrån projektets riktlinjer centralt men det är inte på *länsfilialen*.

1.37 JF: I lagen så är det också en uppmuntran till teknisk interoperabilitet, alltså samarbete men olika branscher eller sektorer. Har ni haft dialog med era konkurrenter eller aktörer i samma bransch för att upprätta samarbete?

1.38 IF1: Den kan jag tyvärr inte svara på.

1.39 JF: Nu har vi lite mer processorienterade eller organisatoriska frågor här. Vad har ni gjort övergripande plan för organisatoriska förändringar på *Företag A* för att kunna erbjuda just dataportabilitet?

1.40 IF: Framförallt är det ju sammanställning och vetskap kring hur i grunden våra processer ser ut i hantering och kontakten i kunddialogen vilken information som hanteras och i vilka register, register som i våra system, som den här informationen finns. Samt vad det är för personuppgifter som finns i respektive register som är då dokumenterad.

1.41 JF: Ni har policies och riktlinjer sen tidigare?

1.42 IF1: Ja.

1.43 JF: Okej. Speciella uppdragsfördelningar också?

1.44 IF1: Nu förstår jag inte riktigt vad du menar med uppdragsfördelningar.

1.45 JF: Nej det kanske är fel ord att säga uppdragsfördelning. Men har ni fått några nya typer av arbetsflöden för de som arbetar med det här?

1.46 IF1: Ja. Här blir nya delar i framförallt i att säkerställa att den information vi skickar till kund är rätt information som skickas till kund utifrån vilken kanal som informationen sänds i. Vi får ju inte skicka känsliga personuppgifter i ett öppet mail, medans andra personuppgifter är okej att skicka i vanlig mailkorrespondens. Så att här har vi ju lite olika tekniska lösningar

för att hantera förflyttningen, hanteringen och bearbetningen av information, i vilken kanal vi ska skicka vad. Det ställer ju krav på kunden också, i förståelse och vilja. Att adaptera ny teknik i antingen dela med sig med kundens information till oss eller att vi ska ge kunden information. Men vi har ju den perfekta kanalen egentligen, det är det inloggade kundmötet. Där är ju informationen skyddad och kunden är definitivt identifierad innan så att det är rätt kund vi kommunicerar med.

1.47 JF: Har det behövs nya processer för att kunna svara på en dataportabilitetsbegäran?

1.48 IF1: Ja men det är väl mer på en övergripande strategisk plan med nya tjänster internt för att vara sammanhållande kring gamla personuppgiftsansvarig till GDPR-ansvarig så att säga. Men det är i grund och botten är det personuppgifterna som vi har i en roll som håller ihop övergripande för att säkerställa att varje enhet i organisationen har uppfyllt sina arbetsmoment på att vara complaint i de olika delarna.

1.49 JF: Vi har också en fråga kring om ni har gjort några typer av anpassningar för att kunna ha gränsöverskridande samarbete med organisationer?

1.50 IF1: Nej det kan jag inte svara på om vi har på det sättet utifrån och försäkrings, bank och liv-engagemang.

1.51 JF: I GDPR så förespråkas även Privacy By Design, är du bekant med det?

1.52 IF1: Ja.

1.53 JF: Har ni förhållit er till det tankesättet eller det ramverk eller strategi när ni gjort nya processer eller tekniska lösningar som tex inför dataportabiliet?

1.54 IF1: Ja helt klart, jag menar banken har levt med de här bitarna länge så det här är inget nyhet i sig. Sen har vi faktiskt inte applicerat några nya systemlösningar i dagsläget så att vi har inte kravställt på den delen, men vi har försökt att titta på hur applicerade lösningar i respektive system verkligen fungerar. Och hur väl förberedda systemen är för att specifikt titta på personuppgiften och logghanteringen kring bearbetningen av personuppgifterna. I det läget så kom det fram att X antal system har vi varit tvungna att uppdatera för att bygga in automatiseringen i de här verksamhetsdelarna.

1.55 JF: Är privacy som design som strategi eller tankesätt något som kommer från högre instans så det blir kanaliserat ner genom organisationen eller är det någonting som man har...

1.56 IF1: Nej det skulle jag inte säga utan det ligger snarare på när upphandlingar görs med integratörerna. Att ställa de kraven rätt i upphandlingen för att som köpare har du inte insyn i design bakom, du ser ett gränssnitt, ett användargränssnitt, men då kan man ju inte se hur den är designad säkerhetsmässigt. Men det vi gör är att tar vi in nya lösningar så gör vi alltid riktiga säkerhetsanalyser av dem med hjälp av tredjepart. För att just hitta de här bitarna att det är kommunikation på rätt sätt, koden är skriven på rätt sätt, hanteringen av identiteter och lösenord är skrivna och programmerade på ett korrekt sätt. Detta gör vi innan vi tar in det och ser vi för stora hål på dessa så säger vi nej eller ber vi leverantören uppdatera eller korrigera och sedan ett nytt test på det.

1.57 JF: Lite generellt vad enligt dig personligen har varit den absolut största svårigheten att kunna erbjuda dataportabilitet?

1.58 IF1: Portabilitet som sagt har jag lite svårt att svara på vad vi exakt har gjort och hur det hanteras centralt för det är outputen av systemen i den leveransen, den kan jag inte idag för vi äger inte utvecklingen av då det ligger som köpta tjänster hos oss. Utmaningen har inte varit sätta processer och skapa regelverk och arbetsinstruktioner för att vara compliant, utan utmaningen är att få medarbetarna i organisationen att förstå varför vi ska göra det detta och vad som landar på mig som individ. Mitt ansvar i hela förloppet i kunddialogen. Så det är nog snarare det som är utmaningen. Vi som jobbar centralt med detta där är det vardagstänk, men medarbetare som svarar i telefon mot kunden eller har personliga kundmöten, där är nog en annan aspekt i att få förståelsen för hur hanterar vi informationen mellan oss med kunden i fokus.

1.59 JF: Hade vi någon mer fråga Edvin?

1.60 EB: Inte vad jag kan komma på. Skulle det finnas möjlighet att få lite klarhet kring filformat på en dataportabilitetsbegäran genom att kolla upp det mot centrala projektet eller är det svårt?

1.61 IF1: Jag tror det är svårt men jag kan ställa en fråga till huvudprojektet och höra.

1.62 EB: Jättegärna tack.

1.63 JF: Annars tror jag inte vi har mer frågor, vi får tacka så hemskt mycket.

1.64 IF1: Tack själva.

Intervju 2 – Magnus Persson – LDC

Intervjuare: Jesper Fransson (JF) och Edvin Blomberg (EB)
Företag: LDC
Informant: Magnus Persson - Informant 2 (IF2)
Roll: IT-säkerhetsarkitekt
Plats: Företagets huvudkontor i Lund
Tid: Torsdagen den 3 maj 2018, 15.00-16.00.

2.1 EB: Okej som sagt, vi har också ett GDPR-fokus men vi har valt att fokusera mer på dataportabilitetsaspekten av det hela. Så vi tänkte att vi köra några inledande frågor. Sen så pratar vi lite om dataportabilitet och sen går vi in på lite mer tekniska frågor följt av lite mer organisatoriska frågor för att sedan avslut. Så första är då, är det okej att vi spelar in?

2.2 IF2: Ja.

2.3 EB: Önskar du vara anonym?

2.4 IF2: Nej.

2.5 EB: Sen tänkte höra lite mer om dig själv, din utbildning och din bakgrund och din roll här på LDC?

2.6 IF2: Jag skulle egentligen bli kemist och sedan halkade jag in på IT-branschen. Det var 1987 kanske. Då läste jag ADB som det hette på den tiden och det är väl det som sen blev systemvetarelinjen för jag såg en del av mina gamla lärare blev lärare på systemvetarlinjen. Så att det var så jag hamnade inom IT och skulle egentligen inte alls jobba med IT men det var mycket mer intressant än det jag höll på med. Så jag hoppade över. Sen har jag jobbat sen 1981 i IT-branschen, först lite grann på privata företag; Tetrapak och securitas och sedan var jag tillbaka på tetrapak igen och sen började jag på universitetet för ungefär 30 år sedan. Då började jag för att jag skulle skriva om LDC:s ekonomisystem, för jag hade jobbat med ekonomisystem innan. Så jag skrev ett ekonomisystem för LDC. Sen när det tog slut skulle man göra någonting annat och då behövdes det lite folk som sålde arbetsstationer och servrar lokalt från universitet från de stora leverantörerna på den tiden som var Digital, Sun, HP och IBM. Så sysslade med det ett tag, sen vill de inte sälja saker längre och då gick jag över till UNIX-support och UNIX-rådgivning men sen tycktes det att det var för få människor som behövde UNIX-support så då halkade jag in på IT-säkerhetsbiten för lite drygt 20 år sedan. Sen efter det har jag jobbat med IT-säkerhet som sagt i lite drygt 20 år.

2.7 EB: GDPR har ju verkligen varit ett ganska stort omställningsarbete. Har du erfarenhet av tidigare omställningsarbete likt GDPR?

2.8 IF2: Ja. Jag var med under milleniumomskrivningen. Det var ju någonting i samma stil. GDPR kan man väl säga är mer omfattande än vad EU hade tänkt sig från början. Jag och många här anser att det här var en lag mer riktigt mot Google, Facebook och de stora och hade kanske inte tankar på att det här skulle bli så omfattande ändå ner till minsta system. Men det har det blivit. Sen är ju Sverige alltid bäst i klassen. Vi kan argumentera massa innan när det ska vara EU-lagstiftning men när det väl kommer till kritan så lyder vi den till punkt och

pricka medans folk längre söderut i Europa kanske inte bryr sig så mycket och sedan när lagen kommer så bryr de sig inte om den. Vi kanske tar det lite mer på allvar också. Men omställningsarbete förutom milleniumbuggen så att säga så är nog det här är en av de största.

2.8 EB: Ja okej. När började ert omställningsarbete mot GDPR?

2.9 IF2: Det började för ungefär för 1.5 år sen, vintern 2016 - början på 2017.

2.10 EB: hur har förändringsarbete i korta drag sett ut?

2.11 IF2: Det har delats upp i två delprojekt. Det första delprojektet körde i ett halvår fram till sommaren 2017. Det skulle ta fram vad vi måste göra organisatoriska, och förbereda inför GDPR. Det var inget tekniskt. Utan hur ska vi ha en organisation som kan fungera i detta omställningsarbete och sen vidare inom GDPR. I detta projektet satt jag med, och sen av olika orsaker vad jag tvungen att hoppa av. Sen var jag med i referensgruppen. Efter sommaren så började mer hands om arbete med migrationen, utbildning, och hur ska vi få reda på vilken information vi har ute. Hur ska forskarna ställa sig till det här? Det var massa verktyg som var tvungna att tas fram. Kontroller av vad vi har och då utbildning av vad som ingår i GDPR-begrepppet. Nu har jag inte riktigt bra koll för det var längesen vi hade ett möte här, och jag hade hoppats på ett möte för det är bara en månad kvar. Ett av resultaten från första delen av projektet var att vi anställde en person som skulle vara informationssäkerhetssamordnare. Denna personen är egentligen den har hand om GDPR, och ansvaret vilar på honom då har han bara jobbat här i 10 veckor. Så han har bara precis kommit in i det här, så en stor del av hans arbete är informationssäkerhetsamordning och sen är det GDPR, alltså att vara personuppgiftsombud så som lagen säger. Detta kommer han jobba med säkert ganska mycket till en början med och sen kommer det säkert minska en del. Därefter kan han ta mer informationssäkerhet. informationsklassning, policys, regelbesult och sånt där.

2.12 JF: Känner ni er redo för GDPR?

2.13 IF2: Vi är inte färdiga, vi är redo. Alltså, Universitetsvärlden har haft stort samarbete de sista året där vi satte upp en maillista där är i princip alla svenska högskolor och universitet med, vilket innebär att vi har samsyn för alla issues kommer upp där. Vi får en samsyn genom detta och därför kommer alla universitet och högskolor göra sin implementering i princip på samma sätt. Därför är detta jättebra för vi står inte ensamma. Vi ser till att vi gör vår inventering, klassificering, beredning, personuppgiftsbehandling, utbildning. Men själva mallen till vad man ska göra kommer vara samma överallt, och då är det lite svårt för datainspektion att peka på att ni ska bötfällas, för då har alla gjort samma fel - och det är lite svårt att säga att alla universitetsjurister i Sverige har tolkat det här fel. Man skyddas lite av mängden av där. Vi är ungefär lika redo som alla andra - dock har ju större universitet mer å göra och längre att gå än lite mindre högskolor. Ju mindre och färskare högskola du är, ju mer central har du på dina grejor. Här är det så fruktansvärt utspritt. Eftersom det i princip gäller allt från ekonomisystem till sekreterarens excelark så är båda personuppgiftsbehandling. Allt det här ska ju registreras på något sätt vilket är en jätteuppgift, och vi kommer inte ha allt på plats, det finns inte en chans. Vi kommer väl inte vara bäst i klassen, men inte sämst, så vi kommer nog vara hyfsat nöjda.

2.14 EB: Har ni använt er av externa konsulter för att genomföra samarbete mellan universiteten?

2.15 IF2: Vi har nog inte haft så mycket annan hjälp utan det har gått mer i excel- och wordformaten att vi har någon såhär datoriserad hjälp på det hela. Och det ser vi ju nu att det kommer oftare och oftare reklam från företag som säger att "vi ska hjälpa er att bli GDPR-compliant". Alltså installera då vårat jättefräcka verktyg här. Jaha, det kostar 12 miljoner om året var det sista jag hörde här sist. Tack vi har inte tolv miljoner att lägga på detta. Dessutom universitet är en så spretig organinsation så här går det alltså inte, rektorns ord är ju ett inlägg i debatten. Folk gör ju ganska mycket som de vill. Varje avdelning har ju väldigt stort eget ansvar och egen frihet och egna pengar. De gör väldigt mycket som de vill. Sen är det ju den här lagbiten och centrala saker som boxar in dem. Men förövrigt gör de som de vill. Därför är det väldigt svårt att införa regler, rutiner och verktyg som är väldigt genomgripande, därför så kommer det att bli lite att man lämnas "ni ska göra såhär och enligt lagen ska ni göra så här och så här" och sen får man väl gå ut på kontroll efteråt och se hur bra det blir och försöka på få in dem i fållan. Men det är ju vår informationssäkerhetssamordnares uppgift och det är ju då dataskyddsombud och det är ju den personen som ska göra audit efteråt och se till att man faktiskt lyder. Men jag menar, låt honom börja börja först. Och lagen gäller inte nu att så att vi har några dagar på oss.

2.16 EB: Som sagt, vårt fokus hamnar lite på en av de större nyheterna, kring dataportabilitet. Är du bekant med dataportabilitet?

2.17 IF2: Japp.

2.18 EB: Erbjuder ni dataportabilitet? Eller måste ni erbjuda dataportabilitet av några uppgifter så att säga?

2.19 IF2: Det beror lite grann på. Alltså den möjligheten att få ut sin data... Alltså om man säger att man vill ha ut sin ladokdata, fine, det får du redan. Då har du redan access till. "Jag vill ha ut all min ladokdata", ja då ska dataportabilitet - vad ska du portera det till? Ett privat ladok? Samma sak där, det här var ju väldigt mycket riktat mot Facebook, Google och Twitter. Att man ska plocka allt som de känner till om dig, alltså vi har inte pratat mycket om dataportabilitet här. För att vi känner inte att, att redan idag har de rätt att få ut den informationen om dig i ett register. Det kan du begära ut, ett visst antal per år du kan begära ut. Så där är ju inte dataportabiliteten annorlunda att bara pratar information, det får de redan ut. Men nu gäller det ju att få ut det på ett sätt eller format som du kan flytta det till ett annat ställe va. Om vi då säger att du ska flytta till ett annat universitet, ja det gör vi redan. Det är ju det ladok är till för framförallt. Och sen resten, ja, vi tar väl ut det ad hoc om det skulle vara så att någon vill plocka ut. Jag kan inte riktigt se att det skulle vara så mycket i våra register som folk vill flytta någon annan stans. Och bara få ut information har man ju fått göra tidigare. Därför tror jag det inte kommer beröra oss så mycket. Jag tror att andra kanske kommer ha större problem, men universitet och högskola känns inte som att dataportabiliteten kommer vara ett sort issue. Och om det händer ja, då tar vi väl ut det och skickar en fil.

2.20 JF: Samlar ni in några interna personuppgifter här på LDC som ni gör någon slags härledning eller avledning på dessa personuppgifter? Profilering eller nåt annat?

2.21 IF2: Nej det kan jag inte direkt säga att vi göra. LDCs roll är ju universitet, vi är en självständiga organisation med vår egen budget. Och vi har inga faster inkomster. Utan allting vi

gör säljs på en köpaSälja-basis. Sen är det vissa saker som är lite svårt att lägga ut på andra, så som skötseln av nätet eller skötseln av telefoni och sånt där. Så vi har lite fasta pengar som vi räknar med att vi ska ha framöver. IT-säkerheten är en sådan. Universitet centralt betalar mig och mina två kollegor som jobbar med IT-säkerhet. Medan andra saker som tex. nu försvann ju driften av LADOK. Det har ju varit mycket pengar in för att vi har ju driftat LADOK åt universitetet här, Malmö Högskola och i princip alla högskolor i södra sverige till stockholm har vi ju driftat här. Det har vi ju kört i våran källare och vi skött driften och betalt till oss. Det är klart att det är pengar in va, men vi kommer nog förlora det eftersom all LADOK-drift kommer ligga på ett ställe och det kommer ligga i molnet. Driftas i Umeå och UDak i Umeå och vi får betala istället för att få in pengar. Så där så LDC fungerar va. Så vi har ju inte direkt något intresse av att göra någon data-mining eller raffinering av data om vi inte har ett uppdrag. För är det ingen som betalar så behöver vi inte göra det. Ja universitet vill ju ha ibland lite datamining, det är inget större direkt. Vi är inte såhär Big Data, söker mönster och allt sådär i stora data mängder, vi raffinerar inte uppgifterna om det inte är en kund som vill ha den. Vi har ju flera uppgifter, den ena är ju drift av system och den andra är då utveckling av system. Båda görs åt kunder, och säger de att de vill göra såhär, ja då gör vi så.

2.22 EB: Men ni på LDC i sig, samlar ni in några personuppgifter?

2.23 IF2: Det är klart att vi samlar in personuppgifter på de som arbetar på LDC. Det måste vi göra. Vi har ju vårt kortsystem för att se vem som kommer in var och vilket rum va. Vi har ett register och lönesystem som är gemensamt för universitetet. Vi har ju lokalbokning här och med personuppgift kontra rum. Det kommer in överallt. Så ja det har vi, men det är inga stora grejer utan det är stödsystem. Alla stora system använder vi ju universitets gemensamma. Så menar vi att vi använder biblar för hantering av anställningsförhållanden och HR-system. Det kommer då flyttas till SSCEA, förutom det så har vi QBiz som är ett litet system som håller reda på var vi lägger tiden. Som sen flyttas över in Paymela så att semestrar och kompledighet blir rätt. Det är litet försystem vi har men det är bara för att vi ska kunna debitera våra kunder, vi har jobbat såhär mycket åt den här kunden och såhär mycket åt den andra. Vilka projekt vi jobbar på, när vi kommer, när vi går och hur många timmar vi jobbar per dag. Så det är litet försystem. Så det är mest de typen av system som LDC själva äger och självdriftar. Eller vi driftar inte ens det faktiskt det är en molntjänst som vi köpt in.

2.24 EB: Vi tänkte ställa lite tekniska frågor men det var också lite i förutsättningen så erbjuder dataportabilitet så det här blir lite mer hypotetiskt i så fall. Om ni skulle få göra....

2.25 IF2: Vi kommer nog få göra det för många kommer testa det här den 26 e maj. Så antar jag att det kommer in en och annan förfrågan. Att bli glömd, tyvärr blir du inte glömd i LADOK. LADOK är ett statssystem, ett system där du inte kan bli glömd. Du kan inte bli glömd i alla system, skatteverket kommer inte radera dig. Så att man ska ta det med en liten nypa salt, alla universitet är statliga myndigheter och då står det i lagen vad vi ska göra så vi har fått ett dekret av regeringen att det här är er uppgift vi ska lösa. Och då måste vi ha ett antal system, och väldigt många är då persondata. De måste vi ha och utan dem kan vi inte fullgöra vår uppgift, alltså har du inte rätten att bli glömd. Vi behöver inte be om lov för att det här är register som man måste hålla och då måste man inte be om lov. Så universitets allmänna ståndpunkt är att det som ger oss problem det är samtycke, vi försöker så långt det går att undvika personregister där det krävs samtycke, vi försöker så långt det går att undvika personregister där det krävs samtycke. Det kommer ju vara sånt som inte är vår kärnverksamhet, det kommer vara fundraisning med externa företag. Det kommer vara alumniverksamhet för studenter som inte längre går här. Bilddata, vi har en bildbank där vi kan använda bilder. Det är

också personuppgifter som vi också måste begära tillstånd för att använda bilderna och sådana saker. Men det är fåtal saker som kommer falla utanför allmänt intresse som det heter. Allmänt intresse är det som vi gör i vår verksamhet som myndighet. Om vi funderar på IT-säkerhet så har vi extremt mycket. Den som har mest loggar vinner när det gäller IT-säkerhet så det gäller att ha så mycket loggdata som möjligt. Som vi i olika sätt matchar i varandra. Och det får man ha. Det är också allmänt intresse, dvs data som krävs för säkerhet för att säkerställa systems drift får man lov att ha utan att be om tillstånd. Så att vi försöker matcha in alla våra register så att... alltså vi lägger de inte i fel kategori för att slippa samtycke. Men vi försöker och se efter var någonstans de ska ligga och då hamnar de nog i princip alltid i någon av de här kategorierna där vi måste hålla ett register. Vissa är avtal tex som anställnings på universitet, alltså får de behandla mina uppgifter då vi har ett avtal och så är du kund/leverantör samtidigt så ger du leverantören rätt att behandla för ni har ett kund/leverantörsavtal. Så det är inte så jättemycket som faller inom samtycke när man tänker efter.

2.26 EB: Just för er verksamhet som är en del av universitetet...

2.27 IF2: Ja mycket av den allmänna, vad som helst, en firma eller ett snickeri eller vad det råkar vara. Deras kundkort eller kundklubb är ett privat person och ett företag och kräver samtycke. Men om du handlar där så kanske är det så.... om du är en större firma som handlar med tillverkare så har ni ju inte avtal. I det avtalet får man lova att behandla personuppgifter. Är du konsult så har du ett konsultavtal, man skriver väldigt mycket avtal innan man gör jobb och i det så finns det då rättigheter att behandla uppgifter. Så vi försöker undvika så mycket det går. Och då underlättar det väl.

2.28 EB: Rent tekniskt vilka utmaningar, enligt dig, har ni ställts inför för att kunna erbjuda dataportabilitet om det skulle komma upp?

2.29 IF2: Eh.. vi har nog inte pratat så mycket om dataportabilitet, ändå litegrann på grund av vi lever i den värld vi lever. Statliga myndigheter lever under offentlighetsprincipen, sekretesslagen ger ju alla medborgare en möjlighet att begära ut i princip vilken handling som helst, och den ska vi plocka fram och det har vi alltid levt efter. Det kan vara så att du vill ha mail från en viss person ur viss tid, eller beslut eller underlag till ett beslut, eller vad det nu råkar vara. Ska man få ut det och det ska ske skyndsamt så att vi har en ganska stor vana att plocka ut information, så vi har alltid levt i den världen att plötsligt kommer det en förfrågan om att nån vill ha all den här informationen. Lundagård skicka en lista med 200 namn där dom säger att vi vill ha, vad var det nu?, jo, cookiefilerna för all dessa personerna, och det ska ske skyndsamt, och skyndsamt brukar vara inom en dag: Nej det kan vi inte plocka ut skyndsamt. Där får man säga att man behöver mer tid. När det gäller register och registerhållning som är IT-baserad så ska det inte vara så jättebesvärligt, då plockar man ut det. Sen beror det litegrann på om vi nu ska lämna ut i ett format som dom vill ha. Vilket format? Vad jag vet så säger ju inte lagen så mycket om format, utan att det ska vara ett portabelt format.

2.30 JF: Precis, vi tänkte gå in på den frågan nu, för det står i GDPR att det ska vara ett strukturerat, allmänt använt och maskininlästbart format.

2.31 IF2: Ja, och jag menar, vi ska skicka i format som XML, JSON eller ett rest-API.

2.32 JF: Det är ingen svårighet?

2.33 IF2: Nej, vi kan skapa en SQL-databas och skicka över. I princip kan vi göra vad som helst. Vi kan skicka en komma-sperarad lista om dom tycker det är bättre.

2.34 JF: Så det finns ingen vidare utmaning när det kommer till just formaten?

2.35 IF2: Nej, det kommer nog komma att vi ställs inför problem. Det är ingenting som jag vet att någon har gjort, tittat efter hur vi ska ta ut information. När jag håller utbildning i GDPR för folk som sysslar med programmering, programmerar system, så säger jag bland annat att privacy by design och privacy by default är viktigt - Du måste kunna radera saker och ting, du måste kunnat fundera ut hur jag ska kunna radera denna personen ur ett system där mycket pekar på varandra så är det inte så himla enkelt att plocka bort, för då kan andra saker faller bort. Hur ska man kunna plockat ut all information? och hur långt sträcker sig den här informationen? Har du en databas, där poster pekar på varandra på många håll, hur långt i hierarkien är den här informationen? Det är inte alltid givet. Då kanske du bara får vad du heter, vilken hårfärg och vilken ögonfärg du har? resten ligger i andra poster. Därigenom är det kanske rätt så ointressant, för då finns det ytterligare poster som pekar på samma sak. Det är ju en mash av information man har, och det står ingenstans var din information står någonstans. Om man frågar Google och Facebook, så kan jag tänka mig att deras datastruktur inte är lättgenomtränglig, och det jag kan begära ut är bara en bråkdel av vad som egentligen finns. För dom måste avgränsa sig lite grann också. Sen måste man förstå vad man får ut.

2.36 JF: Ja, det är också en annan femma.

2.37 IF2: Jag menar, vi kan få ut ett utdrag ur ett register och där kan hårfärg vara 5, skostorlek A. Du har inte indexet till vad dom här betyder. Detta är inte alls ovanligt, man sparar inte saker och ting i klartext. Jag menar, har du färger, vit, gul, röd, då sparar du inte röd i posten utan du sparar siffran 3, som är siffran för 3.

2.38 JF: Precis.

2.39 IF2: Har du inte den här kopplingen förstår du inte vad du får för något. Jag tror inte det står att det ska vara lättbegripligt. Det står att det portabelt i ett format som är allmänt erkänt. Inte att du ska förstå vad du får.

2.40 EB: Lagen nämner lite att det ska vara återanvändbart, lagen pratar om att man ska skicka lite metadata om det går, men det ja, det är som du säger, det är väldigt komplext.

2.41 IF2: Nej, jag tycker som att det känns lite som att dom inte riktigt hur IT-system förstått, eller så är det bara lie spel för galleriet. Ja, du kan få ut lite data, men det finns ingen garanti på att du ska förstå vad du får ut. Även om du får ut det i ett portabelt format, så betyder det inte att du kan läsa in det. Detta eftersom dom har använder andra koder och andra begrepp, så jag betvivlar att du kan plocka ut data från Google och läsa in det i Facebook. Dom har helt olika datamodeller, och om dom inte har någon typ av intergrationsmotor i mitten som kan översätta och modellera om det här till ett vettigt format i andra änden, så vet jag inte riktigt vad man ska göra med det. Det känns som om dom inte har funderat igenom det här, men att detta är ett sätt att sätta press på de stora drakarna. Dom ska inte kunna sitta och samla på sig data om en person i vilken omfattningen som helst. Den här personen har nu rätt att få ut sin data. Även om jag inte förstår min data så har jag har åtminstone fått ut den.

2.42 EB: Lagen själv nämner lite att den vill uppnå någon slags standardformat, och branschsamarbete. Den uppmuntrar till att organisationer ska samarbeta med konkurrenter och inom samma sektor, är det något som ni gjort i dataportabilitetssyfte, finns det någon konsensus kring hur man ska göra?

2.43 IF2: Jag har inte hört något om konsensus i det fallet, jag tror ingen skulle ge sig på att försöka ge sig på att göra detta innan laget tagit kraft. Man vill då se om detta är ett problem, är det inget problem behövs det inte lösas. Är det däremot ett stort problem så beror det på om det är en win-win situation, dvs, jag har lite att vinna på att kunna lämna ifrån mig information i ett standardiserat format för att jag kommer få en hel del information i standardiserat format. Är du däremot i den änden av spektra att du endast kommer lämna ifrån dig information, du kommer inte få in information i ditt system, du är en av de stora drakarna som bara kommer skicka ut data, så finns det ingen orsak att lämna ifrån sig data i det formatet jag har tillgång till - det här är XML, varsågod och läs. Det kan vara svårt att säga hur detta kommer gå. I vissa fall är vissa stora företag jätteglada i att samarbeta, medan i andra fall är det arga konkurrenter. Ett exempel är alla antivirusföretag som samarbetar. Dom sitter runt jorden och analysera där någon tidszoon är vaken, och är det någon som hittar någon i någon tidszoon så skickas det ut till alla andra företag. Alla dessa företag får då samma typ av virusdefinition, alla vinner på det, därför gör man det. När man sen ska sälja saker är man konkurrenter, men ingen orkar göra detta själv så alltså måste man göra detta själv.

2.44 JF: Detta var lite mer av de tekniska frågorna vi hade. Jag tänkte vi hoppar över till lite organisatoriskt och processorienterade frågor. Rent organisatoriskt och processorienterat, vilka utmaningar tror du ni ställts inför om ni nu fått en stor kvantitet dataportabilitetsbegäran?

2.45 IF2: Ja, det är första problemet vore ju att fundera ut vilket format man skulle plocka ut och på vilket sätt man skulle plocka ut det. Jag tror att alla de flesta system vi har här så är det överhuvudtaget inte tänkt på hur information ska plockas ut och i vilket format, samt hur stora del av alla register. Är det bara personposten, är det alla länkar ur posten som ska ut, eller whatever liksom? Det ska ju vara all information om den här person, och det kan ju vara svårt att veta hur långt man ska gå. Jag tror inte folk tänker riktigt på detta.

2.46 JF: Tror det behövs att man upprätta vissa policys, riktlinjer för hur en sådan begäran ska tas emot och behandlas?

2.47 IF2: Ja det tror jag, dock har jag inte läst lagen så noga. Ja, allt detta ska kunna göras men jag vet inte hur fort hur detta måste ske. När det gäller offentlighetsprincipen så är det skyndsamt och skyndsamt beror ju lite grann på hur juristerna tolkar skyndsamt. "Här tolkar jag skyndsamt som väldigt snabbt". Kan du inte svara på en förfrågan på samma dag, i princip, du har max ett dygn på dig och är det inte färdigt så måste man meddela att man tyvärr inte har tekniska möjligheter att ta ut information. Lunds Universitet är väldigt öppet när det gäller vad som ska lämnas ut och hur snabbt det ska lämnas ut. Där tolkar dom det ganska snävt, till vår nackdel och den frågandes fördel, och det kan vara väldigt svårt att få ut data på ett sätt som dom kan använda. Om dom begär ut väldigt stora mailflöden, så måste det gå att se igenom för där ska privata mail plockas bort osv. Nu har vi ju ganska lite som är sektressbelagt, men i mitt jobb finns det saker som är sekretessbelagt: allt som har med lås- och larm att göra är sekretessbelagt, allt som har med patent som inte är färdigtsökt och en del forskning med känsliga uppgifter ska plockas väck. Det kan vara rätt mycket. En massa mail. Detta göra att man kanske inte kan klara det här inom en viss tid, och sen ska det lämnas ut på ett

sätt som den här personen kan läsa, och då kan vi skriva ut de första nio sidorna gratis. Det har ju hänt, då det var en journalist som begärde ut någonting. Det var superbesvärligt att få ut den där informationen. Det blev rätt mycket information och vi behöver inte lämna ut det i elektronisk form, vilket GDPR kräver att man ska kunna lämna ut, men det behöver man inte om man inte vill enligt offentlighetsprincipen. Vi valde att inte lämna ut det elektroniskt, vi sa att det är så här mycket data och vi kommer printa ut det, du kan antingen printa ut det eller komma upp till kontoret och läsa det för hand - eller så kan du printa det och då kostar det si och så mycket - "äh, jag hör av mig". Alltså har vi jobbat en dag i onödan för det här.

2.48 EB: Som du säger, det här är ju ganska likt dataportabilitet då uppgifterna måste bara röra dig själv och liknande. Dessa uppgifter måste ju sorteras, gör ni detta för hand?

2.49 IF2: Ja, om vi kommer göra detta som vi gör enligt offentlighetsprincipen så är det manuellt. Det får man då ta och gå igenom.

2.50 JF: Kan detta automatiseras på något sätt? Det beror ju självfallet på vilken förfrågan det gäller.

2.51 IF2: Om du har system där du får den här frågan upprepade gånger så måste du göra på rutin, för att kunna plocka ut information. Jag kan ju gissa att dom som bedriver större företag kan förvänta sig att få fler dataportabilitetsbegäran. Då får dom nog fixa något jobb som går igenom och plockar ut informationen ur databasen och plockar ut i ett vettigt format. Vi har väldigt massa system (på LDC) och förväntar oss nog inte så väldigt många förfrågningar av denna typ, om vi får några så gör vi dessa för hand, sen får vi titta på resten.

2.52 JF: Ja detta är ju väldigt svårt att se i dagsläget.

2.53 IF2: Jag tror att det kommer bli en puckel med alla jäkla förfrågningsgrejor nu i slutet av Maj, sen kommer semestrarna och då kommer folk lugna ner sig och glömmer det. Sen blir det ett normallägen om ett halvår.

2.54 JF: Vi talade ju om standardisering mellan olika verksamheter, och i ditt fall blir det väl samarbetet mellan olika universitet som du nämnde tidigare. Har ni gjort några anpassningar för att kunna ha ett gränsöverskridande samarbete som GDPR förespråkar kring just dataportabilitetsförfrågningar inom er bransch?

2.55 IF2: Alltså dataportabilitet har inte varit på agendan speciellt mycket. Antagligen för att vi inte tror att något universitet kommer drabbas av många förfrågningar. Det är ju så att de institutioner i landet som har högst kredibilitet, de som flest människor tror på, så är ju universiteten alltid i topp. Folk tror på universitet, vi är good guys, vi är snälla. Vi har hög kredibilitet, ehm, så därför tror jag inte ser oss som första valet om man ska begära ut sin information, för dom litar nog på att vi sköter detta på en ganska bra sätt. Då är det nog mycket roligare med skatteverket eller polisen.

2.56 EB: Den här frågan är inte lika lik de andra, men som du nämnt tidigare. Privacy by design är något du är bekant med?

2.57 IF2: Ja.

2.58 EB: Hur förhåller ni er till PbD som strategi eller ramverk? Tar ni det i beaktning vid utveckling system och processer? Till exempel vid byggandet av dataportabilitet?

2.59 IF2: Jag har lite GDPR-utbildning för dom som är intresserade och för dom som är i det här huset, samt några till ute på universitet, och jag trycker ju på det här. Det är de system vi har som ska gås igenom, man ska titta efter om man hanterar mer information och persondata i detta än som är nödvändigt. Behöver jag då den här datan? Det finns ingen data som är bra att ha när det gäller persondata, utan använder jag den ska jag ha den, annars ska jag inte ha den. Det är även väldigt väldigt svårt att ändra ett system till PbD och privacy by default, men att designa om ett gammalt system med privacy fokus är väl jättesvårt. Men till alla dom som sysslar med utveckling så trycker jag på det. Det är lätta saker att komma ihåg, privacy by design och privacy by default, och uppgiftsminimering, det är dom tre sakerna man ska ha i huvudet. Förhoppningsvis så vet de flesta som ska utveckla saker om detta och följer det. Gamla system är ju ganska svåra att skriva om, och kanske ska man fundera över om man ska radera saker som man använt tidigare men inte använder längre.

2.60 JF: Hur är det med anonymisering? Är det något du förespråkar?

2.61 IF2: Vi har väldigt mycket anonymisering, men det är mest i forskningsavseende. Dels har vi pseudonymisering och då finns det ju ett index någonstans inlåst med försökspersonerna är ju nummer 1, 2, 3 och du kan ju inte förrän du arbetar med materialet veta vem som är vem. Om man forskar på dessa personer och information ska lämnas om dessa över tid så måste samma person matchas med nya svar och då pseudonymiserar man. Vid anonymisering kan du aldrig matcha. Vi har rätt mycket forskning som är väldigt intresserade av att kunna hemlighålla uppgifter som är på ställen man inte kan tro i första hand. Det är folk som forskar på saker och ting och har kontakter med folk i länder med förtryckarregimer, och dom vill kunna kryptera och vill kunna dölja sin information. Dom reser kanske i länder där man inte är säker att en uppgift man har på sin dator är sin egen när man åker därifrån. Därför vill dom kunna ha uppgifterna krypterade och dolda. Där kan det finnas personuppgifter. Jag tror jag kom lite off-topic.

2.62 JF: Avslutningsvis, vad enligt just dig personligen är den största utmaningen med att kunna erbjuda dataportabilitet?

2.63 IF2: Jag kan se ett problem med de system som inte vi driftar, utan t.ex som ligger i molnet. Ska vi ta ut uppgifter ifrån det så kan det kanske bli besvärligt. Då är det flera led som förfrågan ska igenom och då blir det jobbigt. I andra fall så känns det inte riktigt väldigt svårare än när vi tar ut allmänna uppgifter. Allmänna uppgifter ligger ju ofta i datasystem, eller it-system, men ja, dataportabilitet blir en ny sak att lära sig. Offentlighetsprincipen kan ju de flesta även om inte alla kan den till punkt och pricka, men jobbar man på ett universitet så lär man sig förr eller senare, och som man faktiskt måste lyda. Jag tror också det är en utbildningsfråga, folk måste faktiskt veta... ja, alltså, oavsett vilket register det handlar om så måste man kunna lämna ut uppgifter. Om det är t.ex. uppgifter i pappersformat, i ett IT-system, i bildformat eller det är genom (arvsmassa) i forskning. För ett genom är ju en personuppgift. Vi måste ju kunna lämna ut en väldig massa typer av information, hur lämnar man ett genom i ett läsbart format - portabelt.. det finns kanske nån standard eller container för genom.

2.64 JF: Ja, det är en komplex fråga.

2.65 IF2: På företag där jag jobbat så har man ganska bra koll vilka system som finns på företaget. Hyfsat bra. Det har inte universitet. Vi har inte den kontroller. Vi vet vilka centrala system som finns, men här gäller det liksom ner till minsta lilla personuppgift, även i löpande text. Det är liksom rubbet. Detta kommer vi inte ha koll på. Universitet hanterar så väldigt

många olika system och forskar sätter upp egna system, och forskar går inte och ber oss fixa, utan dom sätter upp dom själv. Vårt problem kommer lite grann handla om att vi inte vet allt om alla system vi har. Nu gör vi jätteinventering så att alla system ska inventeras, och det kommer vara jättebra, men kommer generera supermycket tid som alla dessa inventeringar gör.

2.66 JF: Perfekt, då tror jag vi är färdiga här. Vi tänkte också erbjuda dig transkriptionen av intervjun så att du kan titta igenom den.

2.67 IF2: Den tar jag gärna.

2.68 JF & EB: Då får vi tacka så hemskt mycket.

Intervju 3 – Informant 3 – Företag B

Intervjuare: Jesper Fransson (JF) och Edvin Blomberg (EB)
Verksamhet: Elbolag
Informant: Informant 3 (IF3)
Roll: Information Security Manager
Plats: Verksamhetens kontor i Malmö
Tid: Fredagen den 4 maj 2018, 10.00-11.00.

3.1 EB: Bara så det får det på band, är det okej att vi spelar in?

3.2 IF3: Japp, det är okej.

3.3 EB: Önskar du vara anonym?

3.4 IF3: Ja

3.5 EB: Sen undrar vi lite mer om dig själv, vad du har utbildning, bakgrund och din roll här på *Företag B*.

3.6 IF3: Jag är Informationssäkerhetsansvarig för distributionsverksamheten här på *Företag B* i Norden. Jag har en gymnasial utbildning på Tekniska Läroverken här i stan och sen så har jag arbetat med de här frågeställningarna under många många år så att säga. Jobbat mycket inom IT-sidan. Men nu är jag specialiserad inom informationssäkerhetsfrågor.

3.7 JF: Okej. Hur länge här du varit här sa du?

3.8 IF3: Jag varit här sedan 2009.

3.9 JF: Har du någon tidigare erfarenhet av något stort förändringsarbete här på *Företag B* som är i samma skalla som GDPR.

3.10 IF3: Oja.

3.11 JF: Vad hade du för roll i de förändringsarbetena, är det samma som nu?

3.12 IF3: Oftast är ju min roll att vara en kravställare i de här sammanhangen. Uppgiften som jag har delegerad av koncernchefen är ju att väga risker i förhållande till konsekvenser så att säga. Ganska enkelt är det det handlar om, vilken risk står vi inför, vad behöver vi göra för att mitigera den risken och i vilken utsträckning. Hur bredd marginal vill vi ha för att gå på rätt sida av risken ska bli sannolik så att säga.

3.13 JF: Vi hade, till att börja med här, lite generella frågor kring just omställningsarbetet inför GDPR. När började ni ert arbete med att bli compliant.

3.13 IF3: Det kan man säga såhär att, vi har haft PuL-lagstiftningen i Sverige i många år. Det har alltid varit en högt prioriterad arbetsuppgift att följa den lagstiftningen som PuL innebar. Vilket innebär att det är svårt så att säga jämföra, det är såklart att det har tillkommit nya aspekter i GDPR som inte hade i PuL-lagstiftningen. Men jag skulle säga att hela katalogiseringen med vilka behandlingar och vilka personuppgifter som förekommer i respektive behandling och respektive process, det arbetet var ju gjort så att säga, mer eller mindre. Så att

det var ju inte en start från ruta ett. Det tror jag inte det varit för något företag i Sverige men det är klart att det är vissa utmaningar i lagen, rätten att bli glömd tex, när det gäller samtyckereglementet där man får lov att återta det osv. Det är ju skillnader. Och det här nu med dataportatbilitet som tillkommit. Men och andra sidan har vi fått nya verktyg som pseudonymisering och liknande som kan hjälpa oss. Men vad vi har gjort, vad vi har lagt större möda kring är verkligen att sätta oss in i lagstiftarens andemening med det här för att liksom förstå vad som ska skyddas. Det är viktigt att ha det perspektivet så man förlorar det, för läser man lagtexten bokstavligt så kan det ge en dimension som ligger bortom lagstiftaren egentligen hade ansett vara nödvändigt. Det är väldigt viktigt att ha det perspektivet. Sen så är det ju såhär att det är här perspektivet som jag pratar om, det kan man alltid diskutera jurister emellan. Det här måste träda i laga kraft och sen så måste vi ha prejudicerade domar för att veta hur vi ska tolka detta och det kommer de fortlöpande åren att ge oss. Vi pratar med våra kollegor i branschen; Hur hårt ska vi spänna bågen? Hur rigid ska vi tolka lagstiftarens andemening? Det finns fluktuationer kring den tolkingsbilden.

3.14 JF: Skulle ni säga att ni är redo här på *Företag B* inför den 25e maj när det träder i kraft?

3.15 IF3: Vi är så redo som vi kan bli. Sen så tror jag att arbetet kring sådana här frågeställningar upphör ju aldrig. Utan här är det hela tiden att applicera, förändra och förnya. Det handlar ju mycket om att vi vill försöka förmedla kunskapen till den enskilde medarbetaren. Den enskilde medarbetaren har ju ett stort ansvar i det här, hur han ska förhålla sig till arbetsuppgifter och till uppgifter han behöver ta del av i sin tjänsteutövning så att säga. Det är ett fortlöpande arbete och vi kommer säkert att trampa i klaveret i saker och ting men vi gör vad vi kan för att minimera det. Vi har ju en god incidenthistorik till PuL att vi inte har hamnat i situationer där vi har lämnat över uppgifter felaktigen. Men vi är ju inte i en bransch där det är normalt att man har man har behov av att dela personuppgifter vitt och brett. Vi är inte som sjukvården eller som annan, polisiär myndighet eller liknande som har den sortens behov.

3.16 JF: Har ni anlitat extern konsulthjälp för förändringsarbetet eller hur har det sett ut?

3.17 IF3: Ja, det har vi gjort. Men inte alls i den utsträckning som vi hade förväntat eller trott från början. Det har ju varit enormt påtryckning från olika konsultbranscher för att man har ju sett det här som en potential för enorma möjligheter till att tjäna pengar. Men vi har behövt att ta lite hjälp i projektledning och liknande för att hålla ihop saker och ting. Men sen är det svårt för att om man ska kunna svara frågeställningarna kopplat till; hur ser behandlingen ut? Hur strömmar personuppgifterna? Vilka personuppgifter är det som avses? Vilket lagligt stöd har vi att hantera de här? Hur ser gallringsrutinerna ut? Det måste en sakkunnig, det måste ju någon som jobbat med de här uppgifterna under många år svara på, det kan inte en konsult komma in och svara på. Så att därför är det ju svårt att ta in konsulter, där finns ju många i branschen som lovat guld och gröna skogar; köp det här systemet. Våra kollegor, behöver inte säga vilket land, ett annat land i Europa som köpte in ett system för 10 miljoner kronor om det räcker. De trodde då att nuså, nu är vi complaint. Men visst, falsk trygghet.

3.18 JF: Det är ganska lite mer komplext än så.

3.19 IF3: Ja.

3.20 JF: Vi tänkte gå över lite till vårt fokus som är då dataportabilitet. Då tänkte vi först frågan vad det är för typ av personuppgifter som ni samlar in här?

3.21 IF3: Alltså det är ju såhär, vi bedriver ju... Man säga att man kan dela upp vår verksamhet i två ben. Ena benet är en oreglerad marknad, en oreglerad hantering. Precis som du tänker när du säljer eller vad det nu är, du får göra hur du vill. Sen har vi också en mycket mycket kraftig reglerad verksamhet. Vi har lagar och regler som styr saker och ting så att säga. Och just när det gäller den reglerade biten så är det ju krav handlar om att den enskilde kunden, slutkunden, medborgaren i landet Sverige ska så att säga lätt hantera det, det får inte finnas någon form utav av marknadsfördelar. Utan man ska lätt kunna byta sådana här saker. Det har aldrig varit något bekymmer för oss kopplat till dataportabilitet i det hänseendet därför att det har varit lagstadgad under lång tid. Att man ska som kund kunna, med en enkelhet, flytta sitt abonnemang från olika el-leverantör och energileverantörer. Så att där har vi redan i branschen utarbetat en standard kan man säga hur det ska se ut, vad man kan förvänta sig, vilka utgifter som går över. Idag är det såhär att kunden hör av sig till vår leverantörsbytesavdelning och sen så var vi kontakt med leverantörsbyte på det andra bolaget och sen så kvittas uppgifterna och man tar över. Sen är det så finurligt uppdelat i Sverige att vi har förutbestämda områden där man agerar utifrån. Vilket innebar vad vi kallar konsumtionsområde. Där man har konsumtion, där har man slags monopol, så kunden kan ju aldrig förflytta sig därifrån. Vilket innebär att portabilitet blir en ickefråga då det aldrig kommer bli aktuellt. Så har vi lite grann sagt; det här med portabilitet, vad innebär det? Vad kan det betyda? Vi har försökt och tolka lagstiftaren, vad är det man menar med det? Och vi har tolkat det till att det är saker och ting som är väldigt populärt nu då. Det är ju att man, precis som vi eller bränsleindustrin när det gäller fordonsbränsle eller annan industri som livsmedelsindustrin tex, att man försöker addera värde till tjänsten. Vår försäljningsprodukt är ju egentligen ganska tråkig, el, det händer ju ingenting. Det är ju som att titta på färg som torkar, det händer inget. Det är inte ofta kunder är ett dugg intresserade; "men du kanske vill veta hur mycket du förbrukar idag eller i eftermiddag?". "Nae det skiter jag fullständigt i, skicka en räkning bara så är jag nöjd med det". Men vi försöker addera tjänster kring de här sakerna och för lite större kunder och även för kunder som är intresserade och där kan man kanske tänka sig. Att inom det området, om man då har en tjänst där man kan följa min förbrukning och följa om man har bytt värmepanna eller jag har gjort någonting. Vi försöker addera möjligheter att köpa till funktioner, koppla in smarta funktioner i huset som hjälper dig kanske att ändra ditt förbrukningsmönster automatiskt kanske utan att du själv interagerar och följa upp det hur det går. Det möjligtvis skulle kunna vara intressant att ta med mig till en annan nätägare t.ex. Men vi har sagt såhär, att vi... Vi har tittat på XML, hur kan det se ut, vad kan man vara intresserad av och faktiskt, vi har inte ett bra svar på det där. Vi känner att vi får träffas i branschen på något sätt, därför att jag tror att många kunder dessutom... vi har nog möjlighet att om kunden säger att om de vill extrahera den här informationen och ta den med sig. Det kan vi nog ordna, men det står i lagen att den ska vara hanterbart och maskinläsbart och så vidare, det kan vi nog göra. Men frågan är om den nya serviceleverantören som den här kunden vill vända sig till om de kan ta emot det där, det är jättesvårt. Naturligtvis ska man ju inte hitta på en egen standard utan man måste använda vanliga protokoll eller vanliga format på att datamaterialet. Det är vår ambition men mer än så har vi inte lyckas utläsa ur varken datainspektionens eller vad lagen säger kopplat till hur man skulle vilja att det här ska se ut, inom vår sektor ska jag säga.

3.22 EB: Nej, det var lite därför vi kontaktade er för det nämns till och med energiförbrukning i lagtexten till viss del. Då var det den tanken som var aktuell för dataportabilitet.

3.23 IF3: Och det är det jag menar, just när det gäller den biten. När det gäller energiförbrukning och kunna flytta, det är ju ett lagkrav vi har haft under många år för att marknaden ska vara fri, att det ska vara lätt för en kund att byta. Det var ju när man släppte regleringen, 20-

hundra ne nu minns jag inte när det var. Men tidigare är det ju så att där som man hade konsumtion, fick man också handla elen. Men nu så kan man då välja vilken elleverantör man vill helt fritt. Och för att kunna göra det så ska det vara lätt, det ska inte vara såhär när man ringer: "nae det här kommer ta tre månader, du måste skriva på fem papper och det är en jättesvår process" utan det skulle vara lätt för kunden, man skulle bara behöva be om att få göra det och sen skulle det vara bra med det.

3.24 JF: Men då har ni ju nästan erbjudit dataportabilitet under en lång tid?

3.25 IF3: Nja, i alla fall när det gäller den aspekten. Så där är vi liksom hemma, men när det sen gäller de andra bitarna, när man läser på datainspektionens hemsida så pratar de mycket om de stora aktörerna som facebook, den sortens företag. Det är då där man ska få sin information utplockad ifrån. Det är ju inte vår bransch, där är ju inte vi va. Om vi då omsätter det till vi sysslar med, möjligtvis "mina sidor" som vi har till kunderna. Det är ju till närmningsvis, kunden sitter inte och bloggar på vår hemsida och skriver vad de ätit till middag och sånt där. Det är inte alls ändamålet.

3.26 JF: Vi hade en annan fråga om behandlingen av personuppgifter. Om ni då gör någon typ av härledning eller avledning som profilering av personuppgiftssegment för att, ja vad ni har för syfte?

3.27 EB: Datamining...

3.28 JF: Eller försäljning eller vad det kan vara?

3.29 IF3: Den frågan är omöjlig att svara på annat än, för alla företag som har ett vinstintresse, att svara annat än ja. Det är klart att det sista vi vill är att få en irriterad kund som får marknadserbjudanden om alla sorters grejer som man i överhuvudtaget är intresserad. Har vi en kund som har fordonsgas är han kanske helt ointresserad av fjärrvärme osv. Så det är klart att vi har en viss form för riktade reklamerbjudanden och liknande. Och det där är ju, efter när den nya GDPR lagen är det ju fientlig mark. Det där är ju ett minerat område med det här. Så det tittar vi extra noga på nu.

3.30 JF: Skulle du tro, rent spontant, om vi skulle gå över till dataportabilitet igen, räknar ni med många dataportabilitetsbegäran av privatpersoner?

3.31 IF3: Alltså det där är ju en hypotetisk fråga, det kan man ju bara spekulera ikring. Men om man kollar på hur många som begär ett registerutdrag, så tror vi ju att dataportabilitetsfrågan blir mycket färre en möjligt dom som tar registerutdrag. Till en början. Det är en början att förhållandet kommer att ändra sig då man inte har förstått värdet av det just nu. Men svaret är nej, vi tror inte det är så många som kommer fråga om dataportabilitet.

3.32 JF: Vi tänkte gå över till lite mer tekniska frågor. Du var inte på det lite tidigare, men rent tekniskt vad tror du att de största utmaningarna är för er för att kunna erbjuda dataportabilitet?

3.33 IF3: Ja det största utmaningarna är naturligtvis att samla in informationen, på något sätt ringa in vad det är kunden kräver dataportabilitet kring. För att inte göra det här gigantiskt

stort. Man måste också förstå att dataportabiliteten är ju uppgifter som kunden har fört in i systemet. Då är det liksom att göra en avvägning, och i branschen har vi diskuterat ganska så länge kring mätvärdet, förbrukningsmätvärdet. Är det något kunden har matat in? Ja det kan man kanske säga, indirekt har han ju det för han har ju förbrukat det va. Men han har ju inte handgripligen suttit och tryck in information. Om man gör liknelsen med LinkedIn eller Facebook eller de här portalerna. Och det var ju det som lagstiftaren hade tänkt sig tror jag då va. Så att nja, vi är inte riktigt eniga i branschen där, men vi har valt att tolka såhär på *Företag B* om vi nu ska vara lite tongivande i branschen. Så tolkar vi det som ja, det är en personuppgift, själva mätvärdet i alla dess former. Därför det visar ju på en egenskap hos dig som kund. Även om det kanske förvisso är så att man inte kan härleda detta till en fysisk person, därför att det är en familj som bor på den här anslutningsobjektet där mätvärdet äger rum så att säga. Men det kan också vara en person som bor ensam naturligtvis och därför kan vi inte riktigt skilja på det utan därför har vi sagt att alla mätvärden är att betrakta som en personuppgift.

3.34 JF: Lite att helgardera sig kanske.

3.35 IF3: Ja.

3.36 EB: Du var inne på det här lite tidigare också, att GDPR säger ju att formatet bör i strukturerat, allmänt använt och maskinläsbart format. Vilka utmaningar har ni sett kring vilket format ni ska erbjuda dataportabilitet i?

3.37 IF3: Ja det man kan säga det är att, vad vi har förstått det är ju det att vi borde internt... Vi har ju många olika system för att hantera olika saker och kanske har förstått att vi kanske internt enas kring en standard. För att så säga förenkla det. Men än en gång här vädjar vi lite till energimarknadsinspektionen, energimyndigheten, kanske svenska kraftnät. Alla de här myndigheterna utbyter regleringsmodell, hur mycket förbrukar vi just nu, hur mycket produceras? Detta går med olika statsfästa protokoll. Så myndigheterna har varit väldigt duktiga fram tills nu då, att peka på att det är den här standarden vi ska använda. Och lite grann tycker vi att det är myndighetens roll kanske, att ge en fingervisning om att så här borde det se ut. I det här fallet så kan det vara svårt för myndigheten, dem liksom vi och nu ni ställer samma fråga va. Vad är det kunden kommer fråga efter? Ja, ingen aning, vad är de ska begära portabilitet på? Ja ingen aning, deras personuppgifter okej. Då får vi ju tolka det, vi kan skicka ut lista i excelformat, namn, personnumret, telefonnumret och det är det vi har liksom, varsegod. Gapa och svälj. Men det är ju jättesvårt. Men alla dem applikationer där vi tex, det börjar bli mer och mer vanligt även inom vår bransch. Som jag var inne på tidigare, mina sidor att man låter kunden själv kunna styra och ställa och göra kanske köp som är kopplade till sin energileverans. Vi har inte mycket men det kan vara lite sånt som lågenergilampor, vi har gjort samarbete med någon värmepannetillverkare, vi har gjort någon vitvarutillverkare. Och det är möjligt att man då där, kanske kan begära ett utdrag hur man valde sina parametrar kring den här biten, kanske. Så att vi är ju inte det här sociala mediet som lagstiftaren hade i tanken när den pratade om dataportabilitet när man pratar om dataportabilitet.

3.38 EB: Jo, det håller vi nog med om. Men vi diskuterade även om att kontakta facebook vilket vi räknade med att vi får prata med en vägg.

3.39 IF3: Ja det förstår jag.

3.40 JF: I en rekommendation i GDPR är ju att man eventuellt kan bygga ett web-API för sina kunder där de kan gå ut och hämta sina personuppgifter. Är det någonting ni har haft i åtanke eller?

3.41 IF3: Ja det har vi. Det där är ju vågskålen, det är ju en kostnad att bygga de här grejerna i förhållande till utnyttjandegraden och hur man tror den kommer vara. Men jag menar med ett företag som sysslar med det som sin huvudsakliga arbetsuppgift att låta kunder interagera med dem så att säga. För dem tror jag att det är en god affärsidé, att kanske utveckla något sånt verktyg. Sen tror jag att i många sammanhang så när det gäller de här webbportalerna så är det nog så att funktionaliteten är inte långt borta. Den kanske finns redan i viss form men det är bara det att ingen har valt att extrahera den i den här formen eller visualisera den på det viset. Men jag tror att den uppförsbacken kan vara olika lång på olika företag beroende hur pass mogna man är IT-mässigt så att säga.

3.42 JF: Du var inne på det här tidigare om just standardformat och branschstandarder, följer *Företag B* och andra elbolag, alltså har ni någon uppsatt branschstandard för hur ni ska lösa portabilitetsbegäran eller något sammanarbetsramverk?

3.43 IF3: Ja det heter EDIL-formatet, har vi en överenskommelse. Det är det vi använder när vi skickar mätvärden mellan oss. Om det är samma format vi använder när vi skickar leverantörsbyte vågar jag inte säga, men det finns en mycket mycket tydlig utarbetat information-interface uppsättning för att det var ju tvunget. När man avreglerade handeln med el så var ju man tvungen att sätta till en nomenklatur för hur det skulle gå till. För att här har vi kanske distribuerat massa ström till kunder som vi inte sålt strömmen till. Men de kunderna måste vi då tala om för till de som de har köpt strömmen av, hur mycket var det, hur många kilowatt timmar var det? Då måste vi formatera på ett speciellt sätt, det är väldigt strikt hur det ska gå till, hur ofta och när detta ska äga rum. Samma sak så måste vi också tala om för producenten att det var just hans små elektroner som gick i vårt nät till den här kunden, och det är ju ett jävla meklande att få till det. Så där kräver att man, det hade varit enkelt om vi hade haft monopol på hela Sverige, men det har vi inte va då det är många producenter. Så därför har vi ju ur den aspekten, tidigt förstått vikten av att enas kring ett protokoll, hur vi diskuterar och överför den här informationen.

3.44 JF: Intressant! Vi tänkte gå över till lite mer organisatoriska och processorienterade frågor. Rent processorienterat, vilka utmaningar har ni ställts för i samband med dataportabilitetsbegäran? Har ni upprättat som du säger nya riktlinjer eller polycies, hur har ni förberett er?

3.44 IF3: Jag ska vara ärlig och säga såhär, jag ska inte säga att vi har parkerat dataportablitetsfrågan, men jag kan säga att den har kanske nerprioriterats lite grann. Därför att vi känner att, det jag som jag sa tidigare, att vi tror inte att det kommer vara som frågar efter det. Och om de gör det så tror jag att det blir någon form av manuell rutin att ordna till det. Därför har vi inte diskuterat det i så hög utsträckning. Vad vi däremot har pratat om är, precis som jag sa tidigare, att vi försöker hitta metoder som är lika från olika system, om vi nu skulle behöva göra en export dataportabilitetsmässigt. Så att vi inte ska behöva, om vi säger att vi får det i XML från något system och sen får vi det i något annat och i något annat system går det inte tanka hem utan man får ta det som en slags bild, en JPEG bild. Hur ska man liksom begripa det här? Och i någon som kommer det som en accessdatabasdetalj, i nån som excel-format va. Eller som en SQL-förfrågan. Så att där kanske vi måste på något sätt hitta någon snarlikhet. Däremot har vi ju, det är enda så pass kan jag säga, att vi har olika taskforces och dataportabilitet har vi satt ihop som en speciellt taskforceområde.

3.45 JF: Har det funnits utbildningstillfällen internt?

3.46 IF3: Ja det har det gjort, nu har vi precis kommit igång med att utbildas sig i det här. Och det är en viktig del, egenansvaret.

3.47 JF: Ja det var ju det här, har ni gjort några organisatoriska förändringar för att kunna ha ett gränsöverskridande samarbete inom er sektor? För att kunna erbjuda dataportabilitet?

3.48 IF3: Inte mig veterligen än så länge, var och en energileverantör har nog jobbat på kammaren själv. Däremot har vi ju träffat datainspektionen, datainspektionen har ju haft olika seminarier där vi har träffats och pratas om saker om kring, hur vi ska tolka lagen, vad som är deras syn på vad vi ska prioritera och åtgärda osv. Men branschen har inte gjort några närmanden till varandra för att enas kring en viss, faktiskt inte kring GDPR. Annars är det ganska vanligt att vi försöker, när det gäller regleringskrav tex. Eftersom vi är reglerade i stora av verksamheten, så måste vi förhandsvisa och förhandsavisera om hur mycket pengar vi ska tjäna. Och hela den modellen, hur mycket vi får ta betalt av kunden, det försökte man ju enas om i branschen och såna här saker kring vi ska tolka det här. Men det är energimarknadsinspektionen som styr det där va, så visst det förekommer, men just inom GDPR har vi inte faktiskt i branschen haft någon samarbete. Mer än inofficiella möten du vet.

3.49 JF: För det är ju som sagt, GDPR förespråkar, vad de kallar interoperabilitet, samarbete inom en viss sektorn. Så det är intressant att ni snackar samman er, men inte...

3.50 IF3: Precis! Vilket vi har gjort under många år, efter avregleringen var vi nästan tvingade in i den här interaktionen för att åstadkomma den här fria marknaden. Men i övrigt har vi inte sagt ner foten, vi tror ju inte att vi är i en bransch som har enorma GDPR-förändringsmässiga frågor så att säga. Jämfört med andra branscher som är väldigt intresserade av dig som person, vilka vanor du har osv. Det är ju inte vi riktigt. Vi har inte det intresset va. Därför tror inte vi att vi har så mycket, den sortens frågeställning.

3.51 JF: Vi hade en liten annan fråga som har att göra med, vad man kan säga är en strategi eller tankesätt som heter Privacy by Design. Är du bekant med det?

3.52 IF3: Jadå.

3.53 JF: För det är någonting som GDPR också förespråkar.

3.54 IF3: Jo det är det.

3.55 JF: Har ni förhållit er till just PbD när ni har upprättat en ny typ av process eller har ni använt det som något slags ramverk för något förändringsarbete ni har genomfört såsom dataportabilitet?

3.56 IF3: Vi har stärkt den tankegången kan man säga. Eftersom vi är ett energibolag så har man enorm skyldighet mot samhället och vi är styra av säkerhetsskyddslag, vi är styrda av olika författningar kring hur vi ska distribuera energi. Vi är styra av ellagen som säger att du som konsument har en viss rättighet osv. Hur vi ska omkoppla och tillkoppla osv. Det har ju gjort att vårt arbete med att med privacy by design, i det begreppet ligger det här att när man designar någonting, när man tittar på någon ny funktion eller någon ny förmåga så ska man liksom bygga in den här integritetstänket redan från början. Det jag så tidigare då, eftersom vi är styrkta av att vi är en samhällsviktig verksamhet så har vi ju rigorösa krav i vem som har

åtkomst till information, hur informationen ska se ut i nätet, krypteringskrav osv. Så det är inte mycket vi har tweaka, men vi har hittat vissa system kan jag berätta som då har, där man kan säga att systemet i säg har haft en underordnad säkerhetsbetydelse för företaget *Företag B*, men det har varit en stor förekomst av personuppgifter där vi behövt höja klassningen. Samt att lite grann skruva åt säkerhetskraven på dem, men de har varit ett mycket fåtal, det har varit mer rena kampanjverktyg osv.

3.57 JF: För annars kan det vara ganska svårt att modifiera ett redan existerande system...

3.58 IF3: Ja ganska svårt och lätt, det berors ju på. Den svårigheten tror jag, och här tror jag många kanske håller med mig, svårigheten tror jag är störst, inte hos systemet utan hos beteendet hos de som använder systemet. Där har du då oftast den största utmaningen att ändra på. Systemet det kan du bara skjuta till massa pengar så har du bara ordnat med det, eller köpa till en brandvägg eller vad nu gör för någonting, du adderar någon kryptering eller du skapar logiska skikt att informationen är svår att åtkomma från olika håll och kanter eller ha en bra förvaltningsmodell. Men att få beteendet att ändras på är lite värre.

3.59 JF: Ja då är det kanske att man får försöka utbilda i Privacy by Design som tankesätt.

3.60 IF3: Ja precis! Och det är också svårighet då man vill inte heller vara någon slags storebror som säger att vi ser dig osv. Man vädjar ju till sunt förnuft hos alla medarbetare samtidigt som man ska hålla sig inom lagens riktlinjer. Men vad vi försöker göra är att vi försöker identifiera alla processer där vi som arbetsgivare har så att säga, låtit medarbetaren startat en process där han ska behandla personuppgift till att vara annat än laglig, eller följa GDPR. Och att det inte ska vara svårt för medarbetaren att ta sig ur den processen och extrahera information eller behandla information annorlunda som var menad från början. Men vissa medarbetare måste ju för olika ändamål, kunna ändå ha en viss frihet för att göra detta för att kunna hjälpa en kund med en reklamation. Eller hjälpa till i samband med flytt eller vad det kan tänkas vara. Någon som fått en vattenskada och där kanske behöver en extra förstärkning med nätet för det behöver sätta dit någon slags kraftig avfuktare. Och då måste man kunna hantera de personuppgifterna också va, men att förstå när man är klar att så ska man radera dem osv, då det kommer mycket till egetansvar.

3.61 JF: Avslutningsmässigt tänkte vi bara sammanfatta lite, vad tror du personligen har varit den största utmaningen med att kunna erbjuda just dataportabilitet för er?

3.62 IF3: Den största utmaningen är nog att förstå kunden på vad det är dem vill lägga själv i det ordet, dataportabilitet. Jag tror inte kunden egentligen kommer förstå vad det är som de frågar efter och jag kan tänka mig att vi drar slutsatsen och inte bara vi utan branschen drar slutsatsen att kunden frågar efter dataportabilitet så är det en del att han vill flytta ifrån vårt nätområde. Eller flytta ifrån oss som handelskund. Eller också få ut ett utdrag som han själv har bidragit till på de tjänster vi har på olika sätt via webben så att säga. Och när vi har tagit ett utdrag från de tre så är det vad vi förväntar oss för att han ska bli nöjd så att säga. Mer än så gör vi nog inte i dagsläget. Sen får vi se vad myndigheten säger om det i slutändan, eller vad kunden förväntar sig. Jag tror nog att kunden förväntar sig att... Det är ju även de här uppgifterna att kunden har ju rätt att få uppgifter rättade, och det kan man säga såhär; ja men herregud det har vi ju haft i urminnes tider, alla har ju kunnat ringt till oss. Vi är ju de första som blir jätteglada om kunden kan ringa in och meddela att vi fått en ny epostadress det är ju jättebra. Vi har ju aldrig varit en motståndare till, så det är svårt att förstå varför man har skrivit så

i lagstiftaren. Men för att få uppgifter om kring vad man ska rätta måste man först få ett utdrag om vad som finns där omkring. Om sen portabilitetsfrågan, det är nästa aspekt vi har funderat på, det kan ju vara så att portabilitetsfrågan är någonting som en kund aldrig kommer fråga efter. Utan det kanske är den nya leverantören som kommer fråga efter det här. Frågan är hur lagstiftaren, kan man som ny leverantör fråga efter dataportabilitetskravet eller hävda portabilitetskravet för att man har tagit en kund?

3.63 JF: Svårt att säga. Det var nog det vi hade. Vi får tacka så hemskt mycket.

3.64 IF3: Tack själva, det var intressanta frågor.

3.64 JF: Som sagt om du vill ha transkriptionen av det här kan vi skicka ut det till dig.

3.65 IF3: Ja det tar jag gärna.

3.66 JF & EB: Toppen, tack så hemskt mycket.

Intervju 4 – Christer Björmander – Skånetrafiken

Intervjuare: Edvin Blomberg (EB)
Verksamhet: Skånetrafiken
Informant: Christer Björmander - Informant 4 (IF4)
Roll: Förvaltningsledare IT
Plats: Företagets kontor i Lund
Tid: Fredagen den 4 maj 2018, 14.00-15.00.

4.1 EB: Lite inledande frågor bara, så att vi får det på band. Är det okej att vi spelar in? önskar du vara anonym?

4.2 IF4: Du får gärna registrera mig som den som gett dig informationen.

4.3 EB: Vi inleder med lite kring dig själv, lite utbildning och bakgrund och vad du har för roll på skånetrafiken?

4.4 IF4: Ja, jag har väl jobbat mycket de senaste 20 år en med CRM-system. Allt som har att göra med Business intelligence, alla program som har med åtskådlighet att göra, såsom Crystal view och Qlik View. De sista året har det dock varit mycket med GDPR. Jag tycker det är jätteroligt och är väldigt nyfiken kring ert val av dataportabiliteten. Jag upplever det som det svåraste och samtidigt mest missförstådda områdena, det har blivit lite som journalisternas nyhet. Så det känns bra.

4.5 EB: Vad är din titel på skånetrafiken?

4.6 IF4: Jag är förvaltningsledare IT för våra CRM-system, och vi är precis nu och växlar mellan ett gammalt till ett nytt CRM-system. Jag ansvarar för det gamla systemet. Vi håller på ett år med det gamla och håller på att fasa in de nya delarna efter hand. Dessa tar över de sista bitarna från det gamla systemet under kommande år.

4.7 EB: Det var faktiskt min nästa fråga, om du har erfarenhet av tidigare förändringsarbete likt GDPR?

4.8 IF4: Det kan jag nog påstå. Vi lever i en föränderlig värld. Allt vi jobbar med idag är inte det ena likt, från förvaltning till utveckling vilket jag gjort under alla dessa åren. Det är en ständig strid mellan vad som är utveckling och vad som är föråldrat.

4.9 EB: Sen tänkte jag fråga kring omställningsarbetet kring GDPR generellt. När började ert omställningsarbete mot GDPR?

4.10 IF4: Jag kan säga så här; jag började skrika här i mars månad i fjol inom skånetrafiken; nu behöver vi nog sätta igång. Det tog väldigt lång tid innan vi kom igång, och det är vi nog inte ensam om av andra företag och bolag. Många är väldigt sena. Det var väl först efter nyår som många företag och vi själva har satt igång. Vi tycker att vi har kommit väldigt långt i detta jobbet.

4.11 EB: Hur har förändringsarbetet sett ut i korta drag?

4.12 IF4: Vi tillhör ju en förvaltning inom region skåne, så vi har då använt en inventeringslista i excelformat, och den har vi i den definierat vad det är för system och applikationer vi

har. Vi har inventerat vilka personuppgifter vi har, även tillgång till vem som har dessa kopplingar till de bakomliggande systemen och applikationerna vi har. Vi har även gjort en inventering vilka personuppgifter som kan klassas som olika konsekvenser beroende på om dessa uppgifter kommer ut. Vi har gjort ett ganska gediget arbete med det här. Vi har ungefär 120 kända system och applikation och för var dag så har man uppdagat ett nytt litet system eller webbsida, som någon använt. Det växer lite lite hela tiden, dock känner vi oss nöjda med det vi gått igenom. Vi har också en personuppgiftsprincip kring alla uppgifter vi har i alla system. Vi har också koll på flödena, hur personuppgifterna går mellan applikationerna och de bakomliggande system. Egentligen så har vi en systemkarta där vi försökt lägga in flödena av personuppgifter, och hur de rör sig i bakomliggande system. Däremot har vi inte gått djupare, alltså alltifrån DMZ zonen och säker arkivlagring, dock vet vi var vi har alla dessa uppgifter. Det blir så väldigt mycket. Sen har vi också väldigt många leverantörer som vi delar system med, Qlikview är ett sånt typexempel. Vi är väldigt angelägna om att Qlik View informationen som vi lägger i verksamhetsystemet och analysportalen är transparent, samt att vår våra leverantörer såsom tågföretagen och bussföretagen så att de kan se samma sak som oss. Där har vi gjort ett lyft inom hela verksamheten hur vi hanterar det här. Det är alltifrån realtid till intäkter och försäljningsinformation eller vad det nu är. Det är väldigt mycket.

4.13 EB: jag förstå, har ni använt er av några externa konsulter för det här arbetet?

4.14 IF4: Det gör vi, vi har t.ex Stratiteq bland många andra. Sen har vi jobbat med det här under många år och vi har egen kompetens på området. Synsättet om man ska ha den här kompetens brukar diskuteras om den ska ligga på verksamheten eller om den ska vara blandad. Men den bör ju vara blandad, både ur verksamhetsansvar, affärsansvar, sen är det viktigaste instrumentet att ha någon som kan ha analys och verktyg för att hantera åt vilket håll vi ska gå. IT ska stödja det här. Väldigt intressant att jobba med. Detta är ingen nyhet för det har jag gjort sen 2002.

4.15 EB: GDPR är ganska brett som du sa, och du pratade om dataportabilitet som en journalistnyhet, och vi valde att fokusera på dataportabilitet även fast man kan inse att det ligger lite mot Facebook och Google. Det ska ju dock appliceras på samtliga verksamheter. Vad är det för några typer av personuppgifter som ni samlar in?

4.16 IF4: Vi har i princip de vanligaste av person och namnuppgifter och rättsuppgifter, och sen har vi blandad kompott hos oss. Vi har färdtjänst, vi har sjukresor. När det gäller handläggning av färdtjänster så har vi avtal och uppdrag av kommunen där vi har myndighetsutövning. Vi ger dom utredning och bedömningar av vem som är berättigad till färdtjänst och där kommer hälsouppgifter in. Sen har vi har mitt konto, och vi är på väg mot mitt företagskonto, där vi uppgifter om kontoinnehavaren i form av kontouppgifter. Sen håller vi inte mer på bankuppgifter utan det är att vi har ett konto där du kan gå in och betala via olika alternativ. Erbjudande på olika biljetter t.ex. Vi har väldigt brett kring dessa olika bitarna. Dock har vi rätt spann för personuppgifter.

4.17 EB: Sparas det någon resehistorik?

4.18 IF4: Ja, ja vi har historik i respektive applikation som vi har, men det är utifrån de bestämmelser som finns i PUL. Det är ett användaravtal. Det är ju kunden som anger vilka uppgifter som han vill ge ifrån sig. Det är för att man ska kunna genomföra köpen eller tjänsterna, det är det vi har.

4.19 EB: Vad för slags hantering sker av uppgifterna? Du pratade om Qlik View, gör ni härledda eller avledda analyser? Typ profilering eller segmentering?

4.20 IF4: Analyserna är egentligen att vi kan titta på hur bra kunderna är, om man säger så, hur ofta går dom in? hur mycket dom handlar. Det finns tankar om att vi ska införa lojalitetsprogram, ju mer man åker ska man kunna få olika erbjudanden. En viktig bit här är ju att om tåg eller liknande skulle bli inställda eller försenande så har vi ju resegarantin, då kan vi ersätta kunden med ett visst belopp. Det är ju vårt sätt lindra kundens svårigheter, då vi inte äger hela infrastrukturens länkar.. vi sitter i bilkön eller tågkön.

4.21 EB: Är du bekant med rätten till dataportabilitet?

4.22 IF4: Ja, mycket.

4.23 EB: Min nästa fråga är: Erbjuder ni, eller kommer ni erbjuda dataportabilitet till era användare?

4.24 IF4: Det måste vi göra då det är en lag. Däremot är det ofta man pratar om att dataportabiliteten ska ske med hjälp av IT-stöd. Många glömmer bort att det är den andra halva också, de manuella processerna. Hur ser dessa ut? och hur tar man fram uppgifterna? Det är så att säga bäst före datum på dessa uppgifter. Det är du som är personuppgiftsansvarig när du kommer till oss och säger att du vill bli kund hos oss, och då är det du som är ansvarig att ge oss de uppgifterna som göra att vi kan göra dessa tjänster. Plötsligt börjar man då titta på vilka tjänster det gäller. När man börjar tittar på det här kan man undra hur mycket som är kvar när man ställer frågan: hur mycket är det kvar? när man sagt att man vill ha ut sina uppgifter. Hur gör vi nu när vi har en annan laglig grund. Jag tänker att vi har en multikund som är medlem hos oss på Mitt Konto och kanske har färdtjänst eller sjukresor, alltså en bred kundprofil hos oss. Så är det så många andra lagar som faller in i det här. Om du går in på banken och gör en transaktion eller köper något på ICA, så finns det någonting inom bokföringslagen och någon annan lag.. det här kan du inte lyfta ut från banken eller ICA. Du kan inte gå till skatteverket och säga: Lyft bort mig jag vill inte vara här, jag vill bli glömd, vad är det då som egentligen är kvar? Och du har det blivit att många tycker att det är svårt, då behöver man en personuppgiftsansvarig? Men vem är det? Det här alltså jättesvårt. Bara biten att gräva fram alla dessa uppgifter inom 30 dagar är jättesvårt, detta är den absolut största utmaningen vi har.

4.25 EB: Ja, detta verkar vara en stor utmaning. Vad är då den rent tekniskt största utmaningen med att kunna erbjuda dataportabilitet?

4.26 IF4: Det vi skulle vilja ha är ett inventeringssystem, som t.ex ett diariesystem där du kan söka på personuppgifter och framförallt dina uppgifter och där de kommer upp att dessa förekommer i olika applikationer eller system. Då skulle man enkelt kunna få fram var dessa uppgifter finns någonstans, steget efter är att ta reda på vad det är för typ av uppgifter som finns. Då blir det en sån här BIG DATA, och det vill ingen ha, utan här är det att man vill kunna söka på personnummer som är den viktiga länken, den är informationsbäraren för att få fram alla dessa uppgifter. Har du då personuppgifter i löpande text så blir det ju sju gånger svårare.

4.27 EB: Vad för slags personuppgifter skulle vara berättigade dataportabilitet om jag skulle kontakta er?

4.28 IF4: Ja, det är en bra fråga, för det beror lite på vilka tjänster du har utnyttjat. Om man gör det enkelt för sig och säger att du är kund hos skånetrafiken och har kopplat upp dina kontouppgifter. Då kan du få se vilka kontouppgifter du registrerat hos oss i ett utdrag och du kan få möjlighet att rätta dom om du vill och vi kan radera dessa. Dessa är generella principer i våra CRM-system. Uppgifterna kan också vara kopplade till vissa bitar såsom betalningar, att du har betalt med swish eller klarna och där finns det ju kopplingar till andra system där det måste finns verifikation vilken intäkt vi fått. Du måste också kunna verifiera från din bank vilken utgift det gäller även om det är långt bak i tiden. När man jobbat med detta i några år så växer det här väldigt mycket. Jag känner att vi är väldigt ödmjuka kring den här uppgiften då det inte finns några riktlinjer. Det har ju skrivits alla dessa artiklarna men det finns inga riktiga prejudikat på det här ännu, och vi famlar nog alla.. och de svar vi får från Datainspektionen är inte fullständiga.

4.29 EB: Det finns rekommendationer kring dataportabilitet om uppgifter som ska ha för att föras vidare till en annan aktör så ska dessa vara i strukturerat, allmänt använt och maskinläsbart format. Vilka utmaningar har ni uppdagat kring det här? hur har ni ställt er kring det här?

4.30 IF4: Det är inte så lätt beroende på vilket system vi har. Ska det vara CSV-fil eller det ska kunna läsas i klartext, eller du ska själv tyda det? Om du tittar på en person, oaktat vem det är så ska denne kunna se och förstå vad som står på dessa sidor. I min värld går detta bara att se via ett worddokument eller i ett exceldokument. Du ska inte behöva ta detta underlaget och gå till någon annan och fråga om denne kan tyda det som står om mig, utan det ska vara tydligt och läsbart. Det finns ju inte än några standard eller normer om hur du ska föra över dessa uppgifter mellan två olika system. Även om vi sitter här hos oss på skånetrafiken och jobbar med stora system från microsoft och alla andra. Inte där heller kan man skaka hand inom dataportabilitet och föra över dessa uppgifter. Vi kan göra det men det kräver mycket arbete. Vi har ju också ett antal underleverantörer som ska hjälpa till och titta på den här biten, och det på grund att vi har många gamla system. Däremot kompetensen som ska klara DB2 och alla andra program för att lösa det här problemet. Dock har vi tur då vi fortfarande har kvar alla de som utvecklat systemen hos oss, därför kan det här bli lite problem när man ska föra över det här på ett enkelt sätt. Det måste finnas någon rutin. Det här är den första biten, den andra biten är när du ska börja värdera vad det är för uppgifter du ska föra över. Informationen du får i din hand; och du säger att du vill ändra på det här! jag vill ta bort detta! jag vill redigera det här! kan jag lyfta ut detta? hur kan ni hjälpa mig att föra över det här? problemen ligger också i att mottagaren av uppgifterna har andra typer av system. Sen kanske du förekommer i många av alla system vi har och inom region skåne där vi har 800000 system som ligger ute och snurrar. Bara att ställa frågan till ett system är knepigt, dessutom kanske du vill lämna många applikationer, och över tiden kan ditt personnummer personnummer förekomma i olika databaser som inte kommunicerar med varandra. Det blir också väldigt lustigt. Personligen tycker jag att detta är den svåraste delen, hur ska vi hantera detta på ett klokt sätt. Vi ska också ha en rimlig arbetsbörda både ur systemens processer och även de manuella processerna. Vi har ju bara en jättestor uppgift i Maj; ta bort allting i de manuella processerna, excelfiler och annat. Ta bort det här. Försök föra in detta i systemen och har vi inte lyckats med detta så får vi sätta oss ned med verksamhetsansvarig chef och titta på vad vi sparat på den gemensamma katalogen. Vi måste ha full koll på vad för uppgifter vi sparat. Regionen har bestämt sig för att köpa in ett verktyg för den här önskade inventeringen till hösten, så jag hoppas på bättre hjälp.

4.31 EB: Vidare, ger GDPR en rekommendation på att bygga ett Web-API för att förenklat just dataportabilitet, har ni tänkt eller gjort något på just detta?

4.32 IF4: Vi har tänkt på det, men den första frågan är ju i det avseendet: hur vet vi att du är du?

4.33 EB: Ja, det är en bra fråga.

4.34 IF4: Det är den första frågan. Ska vi ha någon form av två-stegs-autentisering? ska vi ha mobilt bank ID? Ska du ha något annat? eller är det så att det är nån släkting eller godman som ska göra detta? Hur vet vi att det med säkerhet är du som frågar? Idag använder vi andra system, och kommer det då någon och frågar: jag vill ha ut mina uppgifter enligt PUL. Då tar vi ut uppgifter och skickar dessa till folkbokföringsadressen. Du får det i ett rekommenderat brev och får hämta ut det på posten utan kostnad och det är vårt sätt att säkerställa att det kommer på folkbokningsföringsadressen. Våra tankar idag är att vi ska ha in ett API och vi ska använda sharepoint. För vår del på skånetrafiken har vi tänkt att om du kommer in med en förfrågan till oss så ska vi försöka lägga in det på sharepoint. Vi har följande system med de här personuppgifterna, så ska det plinga till i min mail där det står att det kommit en förfrågan från dig på ett enkelt sätt. Jag ska kunna enkelt säga att: ja, det är de här uppgifterna det gäller och sen lyfta personuppgifterna till sharepoint för att sen försöka sammanställa de på ett smart sätt. Detta är vår tanke på hur vi ska göra det. Vi tänker i dessa banor men vi är inte där än.

4.35 EB: Vidare står det i GDPR att man uppmuntrar till branschstandarder och branschsamarbete. Har ni haft någon dialog eller har ni satt på någon teknisk branschstandard för uppgifterna som ska skickas vid en dataportabilitetsbegäran?

4.36 IF4: Inte alls. Det vi har gjort är att försöka samarbeta utifrån databaserna som finns, och då försöker vi titta utifrån kundens synvinkel. Alltså vilka kundsystem har vi idag. Och vi har sagt att vi ska titta på de 5-6 viktigaste systemen nu, och det är mobilappen eller mitt konto och det nuvarande systemt BIT-Cubic. Hur ska vi kunna fixa det här och få upp ett API och få fram de här uppgifterna hos oss själva först. Vi är samtidigt i en brytningspunkt där många av de andra trafikföretagen, eller länsbolagen själv hittar på egna biljettsystem som vi nu gjort med vårt biljettsystem. Västra götaland, hallandstrafiken, östergötlandstrafiken och smålandstrafiken ska luta sig mot oss, och plötsligt kan en kund förekomma på många ställen om denne köper en biljett från här i Skåne till Linköping. Dock försöker vi hålla oss till vad vi själva har och försöka hitta personuppgifter, samt försöka minimera rutinerna kring exempelvis pappershandläggning och få allt på burken. Dock har vi alla kundärenden inne i våra CRM-system och dom kan vi hantera.. så det löser vi.

4.37 EB: Nästkommande frågor är lite mer organisatoriska och processorienterade. Vilka utmaningar har ni enligt dig ställts inför för att kunna erbjuda dataportabilitet?

4.38 IF4: Ja, det är ju egentligen inte en IT-fråga egentligen utan en verksamhetsfråga, och hur man ska hantera detta och med vilket IT-stöd som behövs. Detta är den omvända bevisföringen idag som är så viktigt, en åklagare kan komma och bevisa att du är skyldig, men i det här fallet när vi pratar om GDPR och dataportabilitet är det vi som ska visa att vi är oskyldiga. Det är ett helt annat tankesätt än vad man hade förr. Nu är det vi som ska tala om vad vi har för något, och vi ska visa att vi har gjort rätt för oss när vi talar GDPR-aktiviteter. Vi har gjort inventeringar, vi har gjort workshops, vi har gjort riskbedömningar, vi har gjort förslag till åt-

gärder och vi har satt in ett antal kontrollpunkter över tid för att följa upp de åtgärder vi beslutat. Detta för att känna att vi blir compliant på papper, och inte bara i luften, utan verkligen sett till att vi gjort det här. Verksamheten som vi har, med försäljningsavdelningar, tåg- och trafikavdelningar ska känna att dom jobbar med dessa frågor, men i den här organisation har vi en förvaltningsansvarig som jobbar tillsammans med en förvaltningsledare på IT som jobbar med kundkanalerna och en för tåg, och en för affärsområden. Däri försöker vi fånga upp alla dessa olika frågor och sen går vi till den ansvariga verksamhetschefen och säger: det här har vi kommit fram till och hur vi jobbar, ge oss nu en push in hur vi ska jobba vidare och ta beslut. Här kan han inte ta ett beslut om vi inte har rätt beslutsunderlag; det här är vad vi fångat upp. Det knyter ju våra affärsområdeschefer mycket hårdare till den kunddatan vi har överhuvudtaget, och det är ju den största poängen med det här.. då vi kan försöka hantera det här på ett annat sätt än att bara använda den kunddata vi behöver. Vi vill jobba transparent och vidimera allt vi kan.

4.39 EB: Ja precis! Om vi går vidare, som du var inne på lite tidigare. Har ni behövt göra några organisatoriska förändringar i samband med att kunna erbjuda just dataportabilitet? Har ni satt upp nya eller ändrat policys, riktlinjer, nya arbetsflöden eller liknande?

4.40 IF4: Ja, det kan man säga eftersom vi lyder under Region Skåne så har vi fått en massa inriktningar.. så här hanterar du personuppgifter.. så här behandlar du resenärer.. så här hanterar du patienter och så vidare.. Vi har fått nya riktlinjer, men vi har också gått in och ändrat lite i det här. När vi pratar för vår del så är det resenärer i skånetrafiken, där vi fått rätta upp det vi pratat om tidigare, samt andra delar som samtycke. Vår tanke är också att vi ska försöka anställa en kille som är den som kan hjälpa oss och ge ledtråden till vår ledningsgrupp att vara den här dataskyddsombudet, men på lägre nivår: en datacontroller. Han ska både kunna se det ur ett personuppgiftsansvarigt perspektiv men även kunna se det ur ett lednings- och IT-perspektiv. Dessa människor med den kompetensen finns inte idag. Erfarenheten får man inte om man inte jobbat ett antal år inom det här. Vi behöver nån som kan leda oss med de nya bitarna som måste vara på plats.. och följa upp. Nån som kan se alla systemen, alla applikationer, hur personuppgifterna flödar mellan applikationer och system ..och bakomliggande system. Som många har pratat på skånetrafiken så vill dom ha en ekonomicontroller.. jag vill då ha en datacontroller.. som är den som är budbäraren och jobbar fram en annan kunskap. Detta blir ersättaren till dagens BIG DATA-resonemang som man hade för 5 år sedan, som jag anser är helt ute idag.. och även Business intelligence. Det är inte detta som är intressant för det är så jäkla mycket data om det här och då vet man inte hur man ska hantera det.. nu ser jag dock möjligheterna med personuppgifterna som vi får nu via GDPR.. då kommer inte heller kunderna vilja ge så mycket information, dock kommer dom ge såpass mycket information så att vi kan följa dom, hur dom reser, betalar och på vilket sätt samt få ett användaravtal på detta och kunna stödja med olika erbjudande. Då får vi ett helt annat förhållningssätt mellan kund och Skånetrafiken.

4.41 EB: Har ni satt upp några nya processer för just dataportabilitetsbegäran?

4.42 IF4: Nej det har vi inte, vi kan väl säga som så: Vi har studerat de olika lägena, vi har kikat på vad som behövs, vi har gjort den manuella processgranskning och satt de manuella processerna vi behöver. Vi kände att vi var tvungna att kunna svara alla våra kunders förfrågan på samma sätt nu den 25e Maj. Därför hade vi ett möte med affärsområdeschefer och verksamhetschefer som var med hela biten. Det var ett jättebra möte. Så den manuella processen

har vi satt, men det kommer ta tid att få in en systemmässig process. En av de största problemen med ett svara på en begäran är att kunna identifiera kunden, är kunden verkligen den som den utgör sig för att vara? Den här aspekten är jätteviktigt. Den är överordnad allting annat.

4.43 EB: Kommer processen bli automatiserad i framtiden?

4.45 IF4: Ja, så länge autentiseringen sker på ett korrekt sätt. Det kommer ju ta tid att få en automatiserad process som kan fiska upp alla uppgifter från alla system..det kommer nog inte kunna funka, men om du däremot kan lägga en förfrågan där du kan hitta vilka personuppgifter du letar efter.

4.46 EB: Nästa fråga är ganska lik tidigare fråga rörande tekniska standardformat, dock rör sig det nu om organisatorisk standarder. Lagen uppmuntrar till det som kallas interoperabilitet, vilket är samarbete mellan verksamheter i samma branscher och samma sektor, har ni haft dialog eller samarbete kring hur processen ska se ut?

4.47 IF4: Nja, inte mer än hur man utvecklar olika biljettsystem, där har vi dock samtal kring vad det är för uppgifter som man ska kunna överföra nu.. om jag som kund vill kunna åka från skåne till göteborg, och vi sitter med olika biljettsystem.

4.48 EB: Men inte just dialog kring dataportabilietsbegäran?

4.49 IF4: Nja, indirekt blir det ju det eftersom det är personuppgifter vi tar emot i våra system och ger ifrån oss till ett annat system. Informationsbäraren i avseendet blir ju mobiltelefonnumret, då det är det vi ger ut, det är bara den som är identifikatorn i det här sammanhanget.

4.50 EB: Här är en fråga som skiljer sig lite från de andra, men Privacy by Design är ett tankesätt eller strategi som förespråkas i GDPR, är du bekant med Privacy by Design?

4.50 IF4: Ja.

4.51 EB: Hur förhåller ni er till Privacy By Design vid utveckling av nya system eller processer?

4.52 IF4: Idag har vi något som vi kallar för utvecklingsprogram. Vår mobila biljett idag är ju den som vi utvecklar idag inom Singapore, som vi kallar detta projektet, och där jobbar vi med dessa typer av frågor: Hur ska vi göra med de aspekter och frågor som det här tar upp? kan vi formulera, kan vi göra det på vissa sätt för att underlätta för kunden? Det är det vi försöker göra. Kan jag vara privat i de olika delarna, kan jag vara anonym i vissa delar? Där är något vi jobbar hårt med, för att underlätta för oss själva och för att underlätta för kundens bästa. Dock har vi inte kommit så långt som jag önskar att vi hade.

4.53 EB: Lite mer konkret, är privacy by design något ni kommer ha i åtanke om ni ska bygga ett API, eller bygga ett nytt system eller göra en process som samlar ihop uppgifterna?

4.54 IF4: Jag kan väl säga så här, vi har ju gjort den här inventeringen med hjälp av excelmallarna, och allt med konsekvens och beskrivningar med vad som innehåller personuppgifter. Vi har kört workshops där vi har identifierat risker, och vi har kommit med förslag till åtgärder.. åtgärder som till ändring av manuella processer, och då tar jag ett exempel med mailen idag, hur hanterar vi mailen på ett mer säkert och bättre sätt än vad vi gör idag. Mailen får inte bli en plats för lagring av personuppgifter. Höja säkerheten på mailen med att hantera

känslig e-post. Där kan vi ta in verktyg som hjälper oss att höja detta. Mailen och vår websida är ju dom två som är de största oroshärderna. Där måste vi lyfta tröskeln för att säkerställa det här. Vi känner igen och vi vet att vi måste öka hygienen på de här olika delarna. Framförallt gäller det med de manuella processerna, idag är det ju väldigt lätt att skicka ett excelark med personuppgifter oss emellan..eller att man bara tycker på den här länken eller använd sharepoint som vi gjort sen ett eller två år tillbaka. För många av oss som jobbar med GDPR, så använder vi sharepoint.. alla inventeringslistor är bara länkar som jobba över information.. alltså inga mail där personuppgifter kan förekomma. Mycket av det här ju en kulturkrock, för det har ju varit så bekvämt att arbeta med mail, då det var så lätt att använda.. och då är ju kontrollpunkterna så viktiga.. hur ska vi hitta dom här åtgärderna för att bli bättre på att minimera hanteringen av personuppgifter i olika flöden? Jo, genom att det kan se ut så här: Varje Måndag eller Fredag ska du ha kontrollpunker som är återkommande varje vecka, hur ser det nu ut i din inkorg och utkorg? För att minimera att det ligger en massa mail.. för att det får inte hända att vi får en stöld där vi tappar en massa personuppgifter. Därför blir det så viktigt att jobba i förebyggande syfte med brandväggar, nätverk, DMZ, säker lagring, och mellan lager.. och hela vägen. Vad är det för data vi vågar lägga närmast brandväggen innan vi riskerar att bli av med den? Detta är det vi kämpar med idag, men samtidigt får det inte bli för svårt för kunden. Kan vi få in mobilt bankID, så blir det nog bättre. Dock ökar bankID-stölder.. så hur ska vi säkerställa den här minimeringen av personuppgifter? Ja... det finns en hel del fina förslag.. dom man inte ringt på ett halvår dom kan ju läggas i ett bakre lager under en viss period etc, samma sak gäller transaktioner med bankID eller Klarna eller kunder som inte kommer in så ofta. Dom lägger vi lite längre bak.. så dom kan vi lyfta ut när vi säkerställt en högre säkerhet. Jag kan uttrycka mig så här.. vi ska inte skydda slottet utan kungen. Förstår du vad jag menar?

4.55 EB: Ja absolut.

4.56 IF4: Det här synsättet ska vi ha, vi försöka skydda kungen och inte slottet då det är mycket svårare att skydda slottet. Dit vill vi komma, och det gör vi på olika sätt. Indirekt via systemmässiga processer men den viktigaste delen är hur kundtjänst och hur hanterar vår personal och hur hanterar kunden själv sina egna personuppgifter. Det är en viktigt aspekt idag, varje kund är ansvarig för sina egna uppgifter. "Jag bör och skall och ta större ansvar för mina uppgifter". Man ska inte behöva ställa frågan till en verksamhet; "vad har jag för kunduppgifter hos er?" man ska inte behöva ställa den frågan för att man glömt utan istället som en kontrollfunktion... som svar på din fråga: Vi försöker identifiera de olika behoven, men jag vet att vi ska försöka få tag i någon utvecklare som kan vara den som kan hjälpa oss med en systemkarta, flödesbitarna.. hur personuppgifter rör sig.. och dom delarna. Vi behöver tänka mer på det här längre fram över sommaren, och då hoppas jag vi har fått en bättre kravbild på vad vi vill ha. För idag klarar vi att bli compliant i alla avseende då vi har så många andra arbetsuppgifter också.

4.57 EB: som en avslutande fråga: Rent generellt, vad skulle du personliga säga är den största utmaningen med att erbjuda just dataportabilitet?

4.58 IF4: Jag tror att det handlar om att göra klart för personen som frågar; Du kan inte lyfta allt och ta det med dig och bara gå.. för det finns andra bitar av det här med lagar, bokföring eller vad det nu är.. som gör att du inte kan ta med dig det där. Sen ska vi försöka få ut som det bara överhuvudtaget går.

4.59 EB: Det var allt vi hade. Jag kan skicka transkriptionen av hela vår konversation.

4.60 IF4: Ja.

4.61 EB: Annars får jag tacka så hemskt mycket.

4.62 IF4: Tack själv!

Intervju 5 – Johannes Sporre – Kraftringen Energi AB

Intervjuare: Jesper Fransson (JF) och Edvin Blomberg (EB)
Verksamhet: Kraftringen Energi AB
Informant: Johannes Sporre - Informant 5 (IF5)
Roll: Projektledare GDPR
Plats: Företagets kontor i Lund
Tid: Måndagen den 7 maj 2018, 10.00-11.00.

5.1 JF: Först och främst, går det bra att vi spelar in?

5.2 IF5: Jadå.

5.3 JF: Önskar du och Kraftringen att vara anonym?

5.4 IF5: Nej det är lugnt.

5.5 JF: Vi tänkte börja med lite standardfrågor där vi frågor dig om din utbildning och bakgrund?

5.6 IF5: Ja det går bra, kör på.

5.7 JF: Vad har du för akademisk bakgrund eller vad har du för utbildning?

5.8 IF5: Jag är civilingenjör inom maskinteknik. Gjorde mitt examensarbete här. Höll på med effekt-flaskhalsar i nätet och se hur man kunde effektivisera det, om det fanns någon idé att göra det och fram och tillbaka sådär. Kollade hur belastningen låg och vilka det var som hade högst belastning osv. Sen fick jag stanna kvar och har gjort lite olika saker sedan dess. Men framförallt är jag projektledare, har fått en sån projektledarutbildning internbildning här. Jag sitter på affärsutveckling här, men hela avdelningen heter affärs- och verksamhetsutveckling. Då man behövde har några av de här människorna som jobbar med linjeöverskrivande projekten. Vi har ju väldigt olika verksamheter på kraftringen, vi har ju vår el och fjärrvärme och fiber. Men elnät, elhandel och sånt där. Så det finns massor olika regler som gör att man ska hålla isär de här olika då. Men vi har också entreprenad som gör mer grävarbeten och sånt. Och eftersom det är så olika typer av verksamheter så behöver man ändå folk som jobbar linjeöverskridande som alltså jobbar mot alla de här delarna då och håller samman. Det kan bli otydligt vilken linje som ska ha ansvar för ett projektet t.ex. Är det IT eller kundservice som ska ha ansvar om GDPR? I början tyckte man det var en IT-fråga men mer och mer blir det en kundservicefråga vilket man sen inser att det är hela företaget som involveras, alla är påverkade av GDPR. Därför valde man någon som sitter hyffsat neutralt, vilket affärsutveckling är och så har man en mer projektledarroll. Men jag är ingenjör i grunden.

5.9 JF: Har du någon erfarenhet av tidigare förändringsarbete som har varit på samma skala som GDPR?

5.10 IF5: Inte så här, stort inte alls. Men jag jobbade, innan vi blev den här projektet, hade vi en stor omorganisation, och för något år sedan jobbade jag på en annan avdelning som var mer det som blev verksamhetsutveckling som hette projektkontoret. Där jobbade vi mycket med att få en projektstyrningsmodel. Där jag jobbade jag också med förändringsarbete, vi höll projektledarutbildningar och hur man blev projektorienterat på Kraftringen. Man bryter ut sig

från linjeverksamheten och försöker lyfta och bli mer matrisverksamhet. Hur kan vi samarbeta, hur har man samma gemensamma mallar, hur skriver man minnesanteckningar, hur skriver man en beställning, hur gör man en riskanalys. Det var ju en typ av förändringsarbete, jag drev inte det men jag var med mycket i det och höll worksshops osv.

5.11 JF: Lite kring omställningsarbetet kring GDPR generellt. När började ni arbeta på mot det?

5.12 IF5: Jag fick rollen som projektledare i Mars förra året, så vi har jobbat ganska länge med detta. Det började egentligen tidigare, men det var också så att det var tre olika verksamheter som lite krockade i detta. Framförallt fick IT detta som en IT-fråga uppifrån, medans kundservice också fick det då de är de som måste prata med våra kunder som är primära i detta. Sen måste vi också lyfta in att HR, att vi anställda också är en privatperson i detta, vi har också rättigheter gentemot företaget. Så det var tre olika delar i organistionen, där alla tänkte; "det är nog en IT-fråga". Men IT säger "hallå, vi kan bygga upp systemen men vi ansvarar inte vad det är för typ av data det är i systemen". Och då blev det lite körigt, då lyftes jag in i det skedet. Så det fanns ett lite arbete innan.

5.13 JF: Känner ni er redo? Kan du svara på den?

5.14 IF5: Jag tror personligen att det inte finns ett företag i hela Sverige som känner sig redo, jag tror aldrig man kommer känna sig redo. Jag har väldigt länge sett det som vårt arbete med hållbarhet, man blir aldrig färdig med det arbetet. Det är någonting du alltid måste jobba med och utveckla. Och jag tror GDPR kommer vara likadant, det kommer se helt annorlunda ut om fyra år gentemot vad det är idag för det är någonting som vi måste fortsätta med. Det är ny aspekt av hållbarhet kan man säga, eller något liknande, miljö, arbetskvalité och arbetsmiljö osv. Alltså att vi behöver lära oss det här, jag tror det kommer ta tid för alla företag och ställa om i det här avseendet. Jag har ju viljat att få energiföretagen i Sverige, det är vår branschorganisation, gå in och sätta branschstandarder; vad är personuppgifter? Hur ser vi på mätdata? Hur ser vi på de här sakerna? Alltså namn, adress, personnummer och fakturor är ganska tydligt, det är kopplat till en person. Men eftersom vi är el och näts-bolag också så har vi massa olika anläggningar ute, och de är ju snarare knutna till en fastighet. Då har vi egentligen två informationsbärare, vi har en informationsbärare som är knuten till kundnummer, det är privatpersonerna då. Men sen har vi ett anläggningsid också, det är knutet till en fastighet då. Medans kunden kan flytta till nästa fastighet och få ett nytt anläggningsnummer så kommer anläggningsnumret alltid ligga kvar. Då är frågan, vem är det som äger den här informationen i anläggningsnumret egentligen? Är det verkligen kopplat till en privatperson eller är det kopplat till en fastighet. Men fastigheten är ju kopplad till en privatperson. Men var någonstans drar vi den gränsen då? Och det tycker jag fortfarande är väldigt otydligt.

5.15 JF: För det var en av frågorna vi tänkte ställa nu när vi går in på det vi ämnar att undersöka, just dataportabiliteten i GDPR. Då tänkte vi fråga vad det är för slags personuppgifter ni samlar in?

5.16 IF5: Just det. Vi har ju försökt att samla in det i kategorier på något sätt. Om man tar den här definitionen, allt som går att koppla till en enskild person och som kan avslöja något om den. Då blir det väldigt mycket konstiga grejer. Då blir det allting som går att koppla ensamt eller tillsammans kan kopplas till en enskild person, då får ju man all möjlig konstig information. Men generellt sätt samlar vi in uppgifter för att identifiera personen, personnumret och sånt för att veta vem vi har avtal med. Vi har också kontaktuppgifter, adress... Identifierare är

väl då namn och personnummer och sen har vi adress, telefoner och mail. Det är ju de här standard. Men sen så samlar vi in kreditupplysningar för att veta om de kreditvärdiga så att säga. Men det har vi också lagar som reglerar kring det. Vad är det mer vi har? - Vi samlar in mätdata på våra kunder för att kunna debitera dem. Alltså vi har sätt att identifiera dem, sätt att kontakta dem och sätt att bygga upp vår nyttighet eller bevisa våra nyttighet och sätt att informera om denna nyttigheten - alltså fakturor och sånt. Det är väl ikring de delarna. Sen så samlar vi också in kundundersökningar, sen använder vi ju kontaktuppgifter för att göra marknadsföring. Så som alla företag behöver göra för att utvidga och kunna överleva så att säga. Men vi samlar inte så mycket jättekonstiga grejer. Även ärendehanteringsloggar är också sånt som man behöver spara på, om de ringer in och frågar.

5.17 JF: Ja för, vidare när ni har samlat in, den typen av personuppgifter som ni ämnar att samla in. Gör ni då någon typ av härledning eller avledning av de här uppgifterna? Som ni gör någon typ av profilering eller att skräddarsyr grejer till kunden?

5.18 IF5: Det är också spännande med det här med profilering, det här med profilering, så fort vi tar våra 150 000 privatkunder och delar de på mitten så har vi gjort en profilering. Men det gör vi absolut. Eftersom vi har så många olika saker att sälja, är det väldigt stort mål för oss att hela tiden jobba för, om du är elnätskund hos oss vill vi också förstås att du ska vara elhandelskund hos oss. Eller om du är fjärrvärmeskund vill vi självklart att du ska köpa el av oss. Ett mål är man ska få Kraftringen som helhetsleverantör. Så där blir det ju absolut en del profilering. Är det marknadsföring köper vi även in data får externa då. Det finns ju andra källor som man kan, företag som samlar massa på sig information från andra källor, så kan man säga att jag vill ha alla personer som har två bilar t.ex. Där kan man tänka att en av de två kan säkert bytas ut till en elbil, det är något annat vi säljer, elmobilitet. Då kanske man kan köra marknadsföring mot dem och kollar om de vill köpa laddstolpe av oss om de är intresserade av att köpa elbil. Eller vi vill sälja solcell åt några, då man tjäna lite mer pengar än gemene man och har råd med det. Då kanske vi säger; "folk som bor i villa och så ska de tjäna mer än si och så mycket pengar". Men vi går ju inte in i våran kundstock och gör det, den informationen köper vi utifrån.

5.19 JF: Är du bekant med rätten till dataportabilitet?

5.20 IF5: Ja, det är jag bekant med den. Och jag har folk på kundservice som hanterar det åt mig. Så jag är inte superinsatt hur vi löste det men har förtroendet för att det de kommer lösa det hur bra som helst.

5.21 JF: Kan ni erbjuda er kunder dataportabilitet?

5.22 IF5: Nu tycker jag återigen man är i den här situationen, hur definierar vi vad en personuppgift är? Just i dataportabilitet så handlar det också om den datan som kunden har eller den registrerade har tillhandahållit oss. Det är ju det de har rätt till. Då måste vi definiera vilken data som de har tillhandahållit oss. Jag vet att det finns ett exempel från någon utbildning, har man en sån här pulsklocka som jag har, då har man då rätt, jag vet inte om de drog rätten vid pulsslag. Då är då frågan, vem är det då som samlat in pulsslagen då? Är det jag när jag är ute och tränar som samlar in pulsslagen eller är det klockan? Nu äger ju jag den här klockan och då förstår jag att det blir så. Men vi samlar in mätdata från våra anläggningar, anläggningsid. Mycket för att drifta nätet men också naturligtvis också för att debitera. Då är frågan, kommer vi behöva skicka med all data i detta då? För det är vi som äger mätarna, sen har vi ett företag som samlar in det åt oss. Men frågan är, är det den som bor i lägenheten som skapar mätdatan

eller är det vi som skapar för att mäta dem? Så är lite sådana grejer där det blir otydligt. Men enkla svaret på den här frågan är absolut, det gör vi redan. Det finns regler kring detta, alla energibolag är skyldiga att lämna ifrån detta vidare när man byter elhandelsbolag. Det ska vara lätt att byta elhandelsbolag, det är en del av avregleringen och sånt. Det ska vara inte vara en svårighet i det. Det är bara gå in på elskling och så säger att jag vill bara byta så hjälper de dig med det. Och då är vi skyldiga att lämna informationen vidare. Så vi lämnar allt som man behöver för att byta elhandelsleverantör och det finns inbyggt i våra system att göra det automatiskt.

5.23 JF: Nästa fråga handlar om de här personuppgifterna ni håller, vad har ni bestämt att kunden ska vara berättigad att få med sig i en dataportabilitetsbegäran?

5.24 IF5: I dagsläget är det det som krävs för att man ska kunna vara kund hos någon annan. Sen är det ju också så att 2021 kommer man gå över till någonting som heter elhandlarcentrix modell. I dagsläget så har du kontakt med både din elnätsleverantör och din elhandelsleverantör. Men från 2021 någon gång kommer du bara ha kontakt med din elhandlare. Att vi elnätsbolag inte kommer ha någon kontakt med kunderna utan allting går via elhandlaren. Såna grejer regleras otroligt hårt via ellagarna, och det gör det idag också i vilken data man ska lämna och sådana grejer. Så just nu är vi ett läge där hela den här kommunikationen hos energibolagen emellan står inför en jätteförändring, den största sen avregleringen. Den kommer hända inom tre år. Så då tror jag att många energibolag över som jag har varit i kontakt med säger; "vi gör redan det här i väldigt stor utsträckning" just dataportabilitet och inväntar då den här stora förändringen egentligen. Om sen att det nu blir så att folk ändå kommer kräva ut och det kommer visa sig att vi måste lämna mer information, då kommer vi lösa det för hand i sådana fall fram tills dess. Vi har sätt att gå in i våra system hämta ut data så är det ju. Om det sån mätvärden t.ex. då har alla tillgång till mina sidor och där finns dem tillgängliga.

5.25 EB: Om jag skulle vilja flytta min information på "Mina Sidor" till ett annat elbolag, tas det också under dataportabilitet?

5.26 IF5: Ja absolut, men det har vi inte kollat jättemycket på. Eftersom det redan har löst sig i det man behöver ha, sen är det frågan. Jag förstår att man har rätt till saker, men vad är syftet? Vad är syftet med att vi lämnar över våra kundärendeloggar t.ex? Det är ju internt i våra system om hur det har fungerat här och det kanske man vill lämna över till någon annan. Även mätdata, för jag menar om du är elnätskund hos oss skickar vi även mätdata vidare som reglerna säger. Det är någonting som jag tycker branschorganisationen ska ta tag i. Antingen om du är elhandelskund och vill ha, det jag skulle kunna tänka mig att vill är då mätdata bakåt i tiden. Säg att man är elhandelskund hos någon och de erbjuder på att du får ha koll på hur mycket el du har använt. Och så vill de då att du hämtar den datan från den tidigare leverantören. Men vi har inget sätt att föra in det i våra system, vi kan inte föra in den datan. Den kommer ligga som en excelfil på "Mina Sidor" i sådana fall. Vi har inte känt att vi har kunnat göra det. Skulle vi göra en teknisk lösning på att få in t.ex. mätvärden från andra företag från excelfiler. Men det finns ju jättemånga elnätsbolag i Sverige, det är väl 150 olika. Många utav oss har väl samma system, men det är väldigt olika hur det fungerar också och då kanske man får det i massa olika typer av excelark. Det känner jag att det måste skötas centralt. Eftersom vi lämnar över allt som är väsentligt för att det ska fungera redan idag, resterande kommer du få ut i ett excelblad istället för pdf. Men vi kommer inte sorterar upp den och vi har inte syncat med andra energibolag för att det ska fungera. Du kommer få den och kommer kunna

göra någonting med den. Det är alltså ingen PDF. Men vi kommer inte göra så mycket mer och det gör vi när den frågan kommer.

5.27 JF: Räknar ni med många dataportabilitetsförfrågningar från kunder?

5.28 IF5: Jättesvårt. Det handlar mycket om hur man lägger upp det också va. I början så tänkte vi ha en sån på Mina Sidor där man får beställa. Man måste ju garantera kundens identitet och sånt. Vi har ju jättemycket kunder som ringer och säger " jag vill ändra namn och allt det kan vara" men vi har i dagsläget inget system för att garantera att den som ringer in är den som ringer in. Man går in och så lovar man dyrt och heligt att det är jag som är jag och sen begär man någonting. Vi har ju svårt att få tag i personer som det är, det här med anvisningsavtal och sånt, folk som inte anmäler att de har flyttat, eller vill handla egen elhandel för man inte bryr sig om sånt. Det tror jag är ganska vanligt i den här branschen, att det är så. Så då har vi sagt att vi lägger in det på mina sidor och då har vi bank-id för ta sig in där då. Och då har man identifierat sig och då kan man göra en beställning där. Men gör man den beställningen för enkel, "Jag vill beställa detta, detta och detta". Vi vill ju jobba för att; vad är det du vill? Vad är det du vill ha? Vad är det du vill komma åt? Så där är hur man gör den, om man säger "vi kan beställa detta" och ha kryssrutor då tror jag att många gör det bara för att och så vet de inte alls vad det är de kan få komma få ut. Så där försöker vi att få det till mer ett fritextfält så får man beskriva vad det är du behöver och så får vi svara. Man ska naturligtvis ha sina rättigheter, men om du inte vet vad är det du vill ha. Om du inte vet vilka rättigheter är, då blir det såhär; Vem ska definiera det då? Ofta när man hör av sig, så är det ju för att man vill ha ut något specifikt och då kan vi absolut hjälpa dig med det och det hade vi gjort även innan GDPR antagligen. Det finns inga hemligheter så. Vad var frågan från början?

5.29 JF: Det vara bara om ni räknade med att få många förfrågningar kring dataportabilitet?

5.30 IF5: Just ja! Utav våra 150 000 privatkunder tror vi kanske att det är 10 av dem som redan i dagsläget. Vi ägs utav Lunds kommun, vi ligger under offentlighetsprincipen. Vi är redan idag skyldiga att lämna ut offentliga handlingar, där jag i samtal med kundservice vet om att det finns ett tiotal personer som tycker om att begära ut detta i tid och otid. För att de tycker att de har rätt till det, eller för de tycker det är kul, lite rättshaverist sådär. Så de kommer säkerligen begära ut sådär. Men vi laddar inte upp med trehundra man som ska svara på konstigheter sådär. Just nu är det två på kundservice som ska börja på detta. Sen är det också såhär, jo vi drar igång det här den 25:e maj, det är inte alls precis innan semestertid och sådana grejer. Det har man ju lite krångel. Samtidigt som man på IT-håll, man kan ju lämna fullmakter och sånt. Det finns orosmoln här på företaget. Alltså våra kunder är ganska basic, där har vi 14 olika kategorier av personuppgifter som vi identifierat. 10 utav dem får ut ur systemet bara genom att klicka på en knapp. Några får man jobba lite mer med att hitta, vi har ju en del olika system och sådär. Vissa svårare än andra att få ut. Många av systemen är redan uppdaterade inför GDPR. Du skriver in personnummer och så trycker du OK så får du ut det. Men det finns ju orosmoment i kring att t.ex. en fackförening. Många är med i facket och sådär. Och så har vi en jurist till en fackförening och säger "Hej, kan jag få fullmakter av så många som möjligt och så går jag och kollar vad det finns för data på er på olika ställen." Och då får han helt plötsligt en fullmakt att komma med 300 förfrågningar på en gång på ett företag. Det skulle vara otroligt svårt att hantera för oss. [...] HR borde vara den naturliga parten som ansvarar för detta, men HR har koll på en väldigt liten del av de grejerna. IT har koll på ganska mycket och kundservice har också koll på en del. Sen är det systemägare till olika konstiga system som sitter på olika ställen sådär. Så det har varit en ganska stor utmaning, att

försöka pussla ihop det då. Men jag tror att alla där här... Vi har hundra rutiner för de rättigheterna och så har vi människor som sitter specifikt på de här sju olika eller vad det är. Och jag tror vi kommer vara hyfsat förberedda. Men vi kommer inte hitta allt. Men när vi väl får in en fråga och testar, det är då man märker vad som händer.

5.31 JF: Vi tänkte gå in på lite mer tekniska frågor. Vilka rent tekniska tror du är de största utmaningar med att kunna erbjuda dataportabilitet?

5.32 IF5: Alltså just nu, är det nog det jag beskrivit innan. Att vi inte vet hur de andras system ser ut. Men det är ju en väldigt stor utmaning, så stor att vi skiter i det i princip. Skiter i det är lite hårt men, vi skiter verkligen inte i det. Men att vi bedömer det som att det blir, det finns något som heter proportionalitetsprincipen i dataskyddsförordningen också. I det då, när inom tre år kommer det här systemet inte finnas. Ska vi då plöja ner fem miljoner för att sen använda det i två och halvt år och sen så inte använda det igen. Då finns en sån grej. Naturligtvis, hur tar vi emot data då? Visst du har rätt att få flytta datan från ett företag till ett annat, men det måste ju också innebära att vi måste ta emot datan. Och i dagsläget tror jag inte det är något annat energibolag som vill göra på något annat sätt än det vi gör idag egentligen. Sen vet man ju att, beroende på hur man gör tolkningen personuppgifter, så faller ju mer eller mindre saker ute eller innanför scopet så att säga. Sen är det också så här, vad ska vi göra med den datan? Helt plötsligt får data från ett annat nät en ett eget i våra system. Visst att vi har data i våra system för att drifta våra nät, det är därför vi har den datan, för att skapa fakturor och sånt där. Det blir väldigt svårt för oss, vad ska vi ha den datan någonstans? Vi behövde den inte till något annat än att uppfylla ett krav inom GDPR. Nej men det är nog det största, att synka med andra företag.

5.33 JF: GDPR är ju relativt otydligt kring vilka format som man ska använda sig av.

5.34 IF5: Absolut.

5.35 JF: Där står bara att det ska vara strukturerat, allmänt använt och maskinläsbart.Vilka utmaningar har ni uppdagat kring vilka format ni ska använda?

5.36 IF5: Ja, alltså det är jättesvårt att veta. Jag tänker att de allra flesta människor klarar att läsa in Office. Sen är det ju frågan, hu mycket data blir det då? Vi samlar ju in ofantliga mängder data på det här företaget. Men just nu så är har jag nog bara tänkt rent praktiskt att det blir bara ett excelblad, det blir väldigt basic. Som jag tolkar det finns det inget krav på vilken struktur de ska vara på datan utan den ska bara vara allmänt läsbart utan vi skickar iväg en datafil till dem, en csv kodad, alltså kommaformaterad fil med bara massa data på. Så får de göra vad de vill med den datan. Det är ju ändå deras data.

5.37 JF: Det är ju som sagt ett rekommenderat format i lagen.

5.38 IF5: Visst, att skapa en sån och skicka iväg den. Men att få en sån då och göra någonting med den. Det känns otroligt konstigt.

5.39 JF: GDPR rekommenderar också att man eventuellt kan bygga ett web-API för kunder att gå in och hämta data. Men det nämnde du med redan med Mina Sidor.

5.40 IF5: Ja, det har vi redan idag. Något av det första som hände där för ett år sedan var ju att vi delade upp det lite i två. Jag ansvar för det övergripande, hur hanterar vi detta, hur jobbar vi Kraftringen. Ja på Kraftringen, hur hanterar vi personuppgifter? Alltså det här med att,

har jag kundkontakt så ska jag inte ha kvar den kundkontakten i mailen utan den ska in i systemet så att kunden sedan har rätt att få ut den datan vi har på den. Så att det inte sparas massa grejer i mailen och inte någon annan stans. Men sen tar det sitt avtryck också i att vi hade 14 största system också, där vi har alla våra kunder och sånt. Där de direkt gick ut och att vi behöver bli GDPR-kompatibla, vi sätter krav och sådär. Men alla de här stora systemen som hanterar våra kunddata, där har vi ställts krav på att de ska vara GDPR-kompatibla. Och jag tror om ett år så är det inget system som går att säljas om det inte är GDPR-kompatibelt. Och det kommer också finnas behov av system som där det synkar in, så vi också, om det är någon som frågar om en GDPR-kompabilitet så ska det vara inbyggd i alla system vi har. Så man bara skriver in personnummer och så får du ut allting. Då har man också så långt att man har definierat vilken data är tillhandahållen av kunden och vad man har rätt till. Men i dagsläget finns ingen prejudicerad dom som säger "det här är personuppgifter" man vet inte utan då får man chansa lite. Då kan man antagligen gå och stålsätta sig vansinnigt, "nej men vi tror att allt är personuppgifter" och då får du ut precis precis allt. Mitt favoritexempel är GSR, ett nummer som är en sån femtonsiffrig kod vi har för att identifiera vilken mätare som är din. Och den är helt obegriplig, den får inte ens plats om lägger ut dem i ett excelark så avrundas de fyra sista sifforna. Om då jag skickar ut massa data till dig och säger att det här är ditt GSR, det har vi för att identifiera din mätare och således dig. "Va ska jag göra med det här då?" Det finns så mycket data som är helt meningslöst att visa för kunden. Vi säger att vi har anläggningsinformation på dig, vi vet var din anläggning är, hur gammal den är etc. Så det finns jättemycket information där, på varje elnätskund, så ska man skriva, tror jag testade skriva ut och då blir över 100 olika fält man kan ha då. Men då har vi postnummer och adress och sen kan det vara ju var du bor någonstans för att vi ska skicka brev till dig. Men sen kanske det är så att du har en sommarstuga och anläggningsadressen och postadressen inte är det samma. Ska man sen definera allt det här och säga att det här är personuppgifterna vi har på dig och kan ha på dig, då blir det oändligt mycket konstiga grejer. Samtidigt som det är helt ointressant för kunden. De behöver veta att vi samlar in personnummer för att vi gör en kreditupplysning och för att garantera att du är du. Så den information du vill veta. Medans i dataportabilitet eller ännu mer i det här registret så får du bara ut all data. Det finns inget krav på att du ska definiera vad det är för data och vad använder vi den till egentligen.

5.41 JF: Vi tänkte gå vidare in på standardformat. Har ni några egna branschstandarder ni jobbat efter, följer ni något ramverk eller har ni dialog med andra verksamheter i samma sektor?

5.42 IF5: Just det här med dataportabiliten som finns idag, där finns det en standard som används av elbolag i hela Sverige som jag förstår det. Jag är verkligen ingen expert på det så vågar inte säga vad den heter eller så. Men det är verkligen uppstyrt hur det fungerar och det sker i våra system automatiskt. Det är ingenting på kundservice man måste bygga ihop. Det kommer in en begäran, jag vill flytta eller sådär. Då tar man in det i systemet och så skickar man någon fil, kommer inte riktigt ihåg. Så ja absolut verkligen och just i energibranschen blir det väldigt mycket för att det ska bli samma standarder. Större utmaningen blir ju att synka ihop med hela EU och sådär.

5.43 EB: Men när det gäller just dataportabiliet i GDPR, finns det någon uttalad standard eller dialog om ett sådant?

5.44 IF5: Inte mig veterligen. Inte just om GDPRs dataportabilitet så. Men jag tror att det varit så mycket i GDPR att försöka komma på vad GDPR är egentligen. Sen när branschorganisationen säger; "vi tar inte tag i GDPR", ska jag ställa mig själv och kriga som energibolag

när det finns 150 andra som också borde kriga om de här frågorna. Vi borde samlas kring detta, men eftersom våran branschorganisation har i uppdrag att samla oss kring olika frågor väljer att backa ifrån det. Då behöver vi i ett samarbete med andra försöka förstå, hur fungerar era system och hur fungerar våra system. Det blir en väldigt stor grej. Kraftringen valde att inte lägga de resurserna på att driva ett sånt arbete utan vi försöker hitta hur vi klarar oss själva istället. Och så försöker man vara snabbfotad och försöka kunna anpassa eftersom. Eftersom det är så mycket frågetecken fortfarande så säger vi att vi löser det för hand första tiden och sen löser vi det allt eftersom. Vi har identifierat det som ett problem och är beredda och svara på det när frågan kommer. Vi vill veta vad andra tycker också.

5.45 JF: Vi tänkte gå över till lite mer organisatoriska eller processororienterade frågor. Vilka utmaningar enligt dig, har ni ställts inför för att kunna erbjuda dataportabilitet på ren organisatorisk nivå? Har ni upprättat några speciella nya policies eller riktlinjer?

5.46 IF5: Ja alltså, dataportabilitet är ganska djupt ner i GDPR. Så det jag har gjort är att jag har tagit... Först har vi informationsäkerhetspolicy som ligger överst, som också är ganska ny, den antogs bara för några månader sedan. Den är hur Kraftringen ser på säkerhetsklassad information, information överlag och vidare om vi delar ut eller delar ut den i så vidare. Under den så riktlinjer för GDPR, riktlinjer hur vi hanterar personuppgifter. Som vi egentligen borde lägga under informationssäkerhetsdelen då, men eftersom det blir en så specifik lag och så höga böter då om man inte sköter sig är det bra att bryta ut den för att visa datainspektionen. Visa dem att det är såhär vi jobbar med det och vara tydliga med det då. Egentligen hade man kunnat väva in det och bara säga: "att det här täcks av den här meningen och den säger ungefär samma sak." Men blir så jobbigt om man skulle vara tvungen att förklara det, tyckte jag. Den beskriver då hur kraftringens medarbetare ska jobba med GDPR generellt. Det här med att man inte ska spara i mailen och att man ska ha rutiner och riktlinjer som uppdateras. Vem som granskar och interngranskning och efterlevnadskontroll och sånt. Sen rent organisatoriskt, vem är det som ansvarar jo det är ju Kraftringen Energi AB som ansvar som vilket i sin tur håller VDn ansvarig. Men sen så har vi en roll som heter personuppgiftssamordnare kallar vi den som kommer fortsätta det som jag gör som projektledare. Detta för att hålla ihop det då det är så många olika avdelningar på det här företaget som är ansvarig för så många olika delar. Men kunden i helheten är dess ansvar sedan. Under den så visar sen då rutiner hur vi hanterar de registrerades rättigheter. Så det är väl det tredje dokumentet då. Där står ju då alla typer av rättigheter som man kan ha, vad är det 13-22 eller vad det är. Då har vi en för våra kunder och en för vår personal som vi håller på att ta fram nu då. Så i den så kommer det stå tydligt hur det fungerar och vad som ska göras och vad händer om folk hör av sig och vill ha detta såhär.

5.47 EB: Vad blev den största utmaningen med att ta fram den här hela vägen ner till dataportabilitet?

5.48 IF5: Jag tror den största utmaningen varit att hitta vem det är som är ansvarig, eller utse vem som är ansvarig då alla vill trycka det ifrån sig. Jag har under lång tid känt att man säger: det är ju kundservice som hanterar våra personuppgifter, det är ju dom som är i kontakt med kund, men det är ju inte kundservice som bestämmer vilken typ av personuppgifter vi ska på våra kunder. Om vi ska kunna fakturera våra kunder så måste vi ha en viss typ av data, då är de redovisning eller ekonomi som ansvara för det. Om vi har en kundkategori så behöver vi upprätthålla den kundkontakten på nått sätt, eller vilka nyttigheter ska vi samla in. Det är inte kundservice som är ansvarig för vilka kunduppgifter vi behöver, det är ju antagligen försäljning som skapar kundkategorin. Det har varit väldigt svårt att beskriva och förklara för folk

att.. du ansvarar för detta. Man skjuter det ifrån sig. Därför vill jag ha personuppgiftssamordnare.. och det är ju de som inte borde finnas för alla ska ta sitt eget ansvar. I grundläget är det ju en så ny grej så folk kommer inte förstå.. saker kommer falla mellan stolarna. Folk kommer säga: "jag fattade inte det här, och det här är inte mitt ansvar!". Ansvar skulle jag vilja säga är det som fortfarande är lurigast.

4.59 JF: Har ni behövt upprätta nya processer vid en dataportabilitetsbegäran?

5.50 IF5: Ja, det ingår också i de här riktlinjer. Vi har ju väldigt mycket mailkonversationer med vår kunder och allt det här ska i våra system.. och i absolut flesta fallen sker detta, men det är också så att det inte händer. T.ex på affärsutvecklingsavdelningen har vi lite nya idéer, om vi tar ett fånigt exempel: energibranschen har ju varit mycket, vi säljer energi punkt slut.. vi måste utveckla oss så vi har börjat sälja solceller och börjat med e-mobilitet. Där kommer vi i en situation där det fortfarande är under utvecklingen, och mycket av de frågorna som kommer till kundservice kan dom inte svara på, för att det är så nytt.. det är ingen standardgrej. Då kan kunden få direktkontakt med nån på affärsutveckling till exempel, och här på affärsutveckling har vi ingen rutin på att vi ska föra in uppgifterna i kundhanteringssystemen. Då behöver vi bygga upp rutiner för det, men det finns säkerligen.. hela det här med samtycke. Vi måste bygga upp nya rutiner för att se till att folk inte sparar data på hög. Vi har nått som heter L-disk där folk spara allt möjligt bara för att. Man vill ha mycket statistik, sjukstatistik eller försäljningsstatistik eller energianvändningsstatistik.. all sån statistik ska pseudonymiseras.. och det tror jag inte man gör idag. Man vill veta vilken typ av grundkund och istället för att säga att det är privatkund eller företagskund så har man bara namn på alla.. för- och efternamn på alla som är villakunder och sen så ser man att där står ett företagsnamn, och det är så man har koll på vem som är vem. På detta sättet får man inte ha det.. det är mycket basic grejor som måste göras.. uppgiftsminimering kommer det bli mycket av.

5.51 EB: Dom här processerna som ni kan ha behövt ha sätta upp eller redan är på plats, är några av dom automatiserade? eller är det tänkt att dom ska bli automatiserade?

5.52 IF5: Vi har jobbat simultant med något som heter Kraftringens processer där man då ska definiera hur man gör något. Sen för man in det i något som heter.. ja vad hette det? 2C8 tror jag det hette. Där ser man om man får en viss fråga så ska man göra på ett visst sätt. Tanken är att detta i längden ska tas in i våra system.. och då är det så här vi gör och sen ska man uppdatera den här en gång i halvåret eller en gång om året. I den uppdateringssnurran måste vi få in GDPR-frågorna: har vi ändrat processen på något sätt och hur har det påverkat hur vi samlar in vår personuppgifter? har vi samlat in något ny typ av personuppgift? men det kommer antagligen börja med om det har påverkat vår hantering av personuppgifter: Ja eller Nej - får du ett Ja, då ska du göra de här grejorna. Det här är vårt mål som vi hoppades att vi skulle hinna med i början men det tog lite för lång tid, för vi behövde sätta oss på plats först. Tanken är ändå att vi ska hinna i mål.

5.53 JF: Har ni gjort några specialla anpassningar för att ni ska ha ett gränsöverskridande samarbete med t.ex. både konkurrent och de som ni samarbetar med inom sektorn?

5.54 IF5: Ja, dels är vi med i olika samarbeten då vi har system.. alltså om vi har ett extern företag som bygger ett system för hantering av personuppgifter på olika sätt, så säljer ju dom det också till andra företag. Det är ganska många energibolag som har samma typ av system.. där vi i vanliga fall har samarbeten.. alltså man har en slags ägandeförening där man driver förändringsarbete via andra företag.. i IT-utveckling. Jag var också med energidataföreningen

där man pratar om hur man lagrar och arkiverar saker.. där lyfter dom upp ett samarbete energibolagen emellan. Dom valde ett annat system för register eller behandling nu i samband med GPDR än vad vi valde.. deras system utgick från vilka system vi redan hade.. men jag ville ha ett system som utgick från vilka kunder man hade. Därför gick vi isär.. dock var det mycket samarbete där vi delade policys med varandra och sånt. Samtidigt var det så här: Hur fungerar era system? Dom kanske hade ett system som stämde och två som inte stämde och var lutar dom i detta? Man fick lära sig mer hur deras verksamheter fungerade.

5.55 EB: Vidare, nästa fråga handlar kring Privacy by Design. Är du bekant med det?

5.56 IF5: Absolut!

5.57 EB: Hur förhåller ni er till Privacy by Design som strategi eller ramverk när ni utvecklar nya system eller processer? Något som har tagits i åtanke kring dataportabilitet?

5.58 IF5: Nu kände jag att jag svarade lite snabbt här, men vi har ju en hel avdelning som jobbar med säkerhet.. vi har ju en anställd som jobbar som informationssäkerhetsansvarig, så vi jobbar väldigt mycket med detta. Sen har vi massa viktigt data i våra system som inte får lämna husets fyra väggar. Vi har ju tagit in jurister som ställer höga krav på våra systemleverantörer.. men vi har ju jättemånga system som köps in för att göra nån mindre grej och på dessa har vi inte den tunga granskningen.. men vi jobbar mycket på det och vi har en avdelning med fyra anställda som bara jobbar med säkerhet. Inte bara personsäkerhet utan också datasäkerhet så vi tar det väldigt seriöst. Och vi ställer höga krav på integritet och säkerhet i de system som hanterar våra kunder och anställda.

5.59 EB: Som avslutande fråga.. vad är enligt just dig personligen den största utmaningen med att kunna erbjuda dataportabilitet?

5.60 IF5: Det är nog att man behöver synka med andra företag och att dom som jag tyckte skulle göra det.. inte gjorde det.. alltså att branschorganisationer borde ta tag i det här och säga: vi anser att det är dom här grejer inom dataportabilitet som borde göras. Dom skulle bjudit in 10 olika energibolag som sätter sig i ett rum i 3 timmar vad gå igenom vad som anses vara personuppgifter och vad ska vi skicka och hur ska vi ta emot detta. Det borde man egentligen kunna lösa på tre veckor men man valde att inte ta tag i det. Vilken data förväntas det av oss? Jag menar; om jag som kund kommer och säger; jag vill ha ut den data jag har rätt till! Då vet inte vi vilken data du har rätt till, och du vet inte det heller.. hur ska du som kund kunna granska oss att du fått med dig rätt data? och sen flyttar du ifrån oss och får med dig en typ av data, och sen flyttar du ett år senare till ytterligare ett nytt företag och får med dig annan data för dom har tolkat det på ett annat sätt. Det är nog samarbetet som är det viktigaste. Det har söks men det har inte funnits.

5.61 JF: Då tror jag inte vi har fler frågor. Då skulle vi såklart vilja erbjuda transkriptionen av intervjun om du vill ändra något, eller stryka något som du sagt eller vi sagt. Om du vill ha det kan du få det.

5.62 IF5: Nej tack det är bra.

5.63 JF: Då får vi tacka så mycket.

5.64 EB: Ja, tack så mycket.

Referenser

Adams, Tim. 2018. Facebook's week of shame: the Cambridge Analytica fallout. The Guardian. Hämtad 2018-04-10 från https://www.theguardian.com/technology/2018/mar/24/facebook-week-of-shame-data-breach-observer-revelations-zuckerberg-silence

Allen, D. K., Karanasios, S., & Norman, A. (2014). Information sharing and interoperability: the case of major incident management. European Journal of Information Systems, 23(4), 418-432. doi:10.1057/ejis.2013.8.

Cavoukian, A. (2012). Operationalizing privacy by design: A guide to implementing strong privacy practices. Information and Privacy Commissioner, Ontario, Canada. http://www.cil.cnrs.fr/CIL/IMG/pdf/operationalizing-pbd-guide.pdf

Chen, D., & Daclin, N. (2006, March). Framework for enterprise interoperability. In Proc. of IFAC Workshop EI2N (pp. 77-88). http://chen33.free.fr/M2/Elearning/CIGI2009.Chen.final.pdf

Datainspektionen, 2017a. Riktlinjer om rätten till dataportabilitet - Vägledning från 29-gruppen. Hämtad 2018-04-11 från https://www.datainspektionen.se/Documents/Riktlinjer%20om%20r%C3%A4tten%20till%20dataportabilitet.pdf

Datainspektionen, 2017b. Riktlinjer om rätten till dataportabilitet - Bilaga med frågor och svar. Hämtad 2018-04-11 från https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registrerades-rattigheter/dataportabilitet/

Datainspektionen, 2017c. Vad är en personuppgift? Hämtad 2018-04-11 från https://www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/vad-ar-en-personuppgift/

Datainspektionen, 2017d. Personuppgiftsansvarig. Hämtad 2018-04-17 från https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/skyldigheter-for-de-som-behandlar-personuppgifter/personuppgiftsansvarig/

Datainspektionen, 2017e. Skyldigheter för de som behandlar personuppgifter. Hämtad 2018-04-17 från https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/skyldigheter-for-de-som-behandlar-personuppgifter/

Datainspektionen, 2017f. De registrerades rättigheter. Hämtad 2018-04-17 från https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registrerades-rattigheter/

Datainspektionen, 2017g. Personuppgifter och personuppgiftsbehandling. Hämtad 2018-04-17 från https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/tillampningsomrade/personuppgifter-och-personuppgiftsbehandling/

Datainspektionen, 2017h. Dataskyddsförordningens syfte. Hämtad 2018-04-19 från https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/introduktion-till-dataskyddsforordningen/dataskyddsforordningens-syfte/

Datainspektionen, 2017i. Introduktion till dataskyddsförordningen. Hämtad 2018-04-19 från https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/introduktion-till-dataskyddsforordningen/

Datainspektionen, 2017j. Samarbete inom EU.
Hämtad 2018-04-19 från https://www.datainspektionen.se/dataskyddsreformen/samarbete-inom-eu/

Eriksson, O., & Goldkuhl, G. (2013). Preconditions for public sector e-infrastructure development. Information And Organization, 23(3), 149-176. doi:10.1016/j.infoandorg.2013.04.001

Everson, E. (2017). Privacy by design: Taking ctrl of big data. Cleveland State Law Review, 65(1), 27-43.
https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/clevslr65&id=31

European Data Protection Supervisor - EDPS. 2018 The History of the General Data Protection Regulation. Hämtad 2018-04-25 från https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Gürses, S., Troncoso, C. and Diaz, C., 2011. Engineering privacy by design. Computers, Privacy & Data Protection, 14(3).
https://lirias.kuleuven.be/bitstream/123456789/356725/1/article-1542.pdf

Harmon, P. (2014). Business process change. Waltham, MA: Morgan Kaufmann.

Hsu, Tiffany. 2018. For Many Facebook Users, a 'Last Straw' That Led Them to Quit. The New York Times.
Hämtad 2018-04-10 från https://www.nytimes.com/2018/03/21/technology/users-abandon-facebook.html

IEEE (1990). IEEE Standard Glossary of Software Engineering Terminology. IEEE Std 610.12-1990. IEEE , Technical report, IEEE, s. 1-84. doi:10.1109/IEEESTD.1990.101064

Jacobsen, D. I., Sandin, G., & Hellström, C. (2002). Vad, hur och varför : om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen. Lund : Studentlitteratur, 2002 (Lund : Studentlitteratur).

Kubicek, H., Cimander, R., & Scholl, H. J. (2011). Organizational interoperability in e-government: lessons from 77 European good-practice cases. Springer Science & Business Media. https://lirias.kuleuven.be/bitstream/123456789/356725/1/article-1542.pdf

Moran.,J.W, & Brightman ., B.K (2000). Leading organizational change. Journal Of Workplace Learning, (2), 66. doi:10.1108/13665620010316226.

Ogelid, Håkan. 2017. EU:s dataskydd – risk för ny millenniebugg. DF Analys. Hämtad 2018-04-23 från http://dfanalys.se/2017/01/13/eus-dataskydd-risk-for-ny-millenniebugg/

Ray, E. T. (2003). Learning XML. [Elektronisk resurs]. Sebastopol, Calif. ; Farnham : O'Reilly, 2003. https://www.dawsonera.com/readonline/9780596516826

Reddy, M. (2011). API Design for C++. Burlington: Morgan Kaufmann Publishers.
https://www.sciencedirect.com/science/book/9780123850034

RSM i Sverige. (2017, Nov 16) *92 procent av Europas företag är inte förberedda för GDPR [Press release]*
Hämtad 2018-05-09 från https://news.cision.com/se/rsm/r/92-procent-av-europas-foretag-ar-inte-forberedda-for-gdpr,c2393169

Schaar, P. (2010). Privacy by design. Identity in the Information Society, 3(2), 267-274.
https://link.springer.com/article/10.1007/s12394-010-0055-x

Shafranovich, Y. (2005). Common format and MIME type for comma-separated values (CSV) files. https://tools.ietf.org/html/rfc4180

Sveriges Radio. 2018 55 000 svenskar drabbade av Facebookskandalen. Hämtad 2018-04-10 från http://sverigesradio.se/sida/artikel.aspx?programid=128&artikel=6924763

Tankard, C. (2016). Feature: What the GDPR means for businesses. Network Security, 20165-8. doi:10.1016/S1353-4858(16)30056-3.

Todnem By, R. (2005). Organisational change management: A critical review. Journal Of Change Management, 5(4), 369-380. doi:10.1080/14697010500359250.

Zhao, K., & Xia, M. (2014). Forming interoperability through interorganizational systems standards. Journal Of Management Information Systems, 30(4), 269-298. doi:10.2753/MIS0742-1222300410.